

**UNIVERSIDADE FEDERAL DA PARAÍBA – UFPB**  
**CENTRO DE CIÊNCIAS JURÍDICAS – CCJ**  
**COORDENAÇÃO DE MONOGRAFIAS**

**LARA GALIZA DE CARVALHO**

**A PROTEÇÃO DOS DADOS PESSOAIS À LUZ DA NOVA PERSPECTIVA DE  
CONSTITUCIONALIZAÇÃO DO DIREITO CIVIL**

**SANTA RITA**

**2017**

**LARA GALIZA DE CARVALHO**

**A PROTEÇÃO DOS DADOS PESSOAIS À LUZ DA NOVA PERSPECTIVA DE  
CONSTITUCIONALIZAÇÃO DO DIREITO CIVIL**

Trabalho de Conclusão de Curso apresentado  
ao Curso de Graduação em Direito de Santa  
Rita do Centro de Ciências Jurídicas da  
Universidade Federal da Paraíba como  
exigência parcial da obtenção do grau de  
Bacharel em Direito.

Orientador: Dr. Adriano Marteleto Godinho

**SANTA RITA**

**2017**

Carvalho, Lara Galiza de.

C331p      A proteção dos dados pessoais à luz da nova perspectiva do  
constitucionalização do Direito Civil / Lara Galiza de Carvalho. – Santa  
Rita, 2017.  
71f.

Monografia (Graduação) – Universidade Federal da Paraíba.  
Departamento de Ciências Jurídicas, Santa Rita, 2017.  
Orientador: Prof<sup>o</sup>. Dr. Adriano Marteleto Godinho.

1. Privacidade. 2. Intimidade. 3. Humanização. 4. Tecnologia da  
Informação. 5. Dados Pessoais. I. Godinho, Adriano Marteleto. II. Título.

**LARA GALIZA DE CARVALHO**

**A PROTEÇÃO DOS DADOS PESSOAIS À LUZ DA NOVA PERSPECTIVA DE  
CONSTITUCIONALIZAÇÃO DO DIREITO CIVIL**

Trabalho de Conclusão de Curso apresentado  
ao Curso de Graduação em Direito de Santa  
Rita do Centro de Ciências Jurídicas da  
Universidade Federal da Paraíba como  
exigência parcial da obtenção do grau de  
Bacharel em Direito.

Orientador: Dr. Adriano Marteleto Godinho

Banca Examinadora:

Data da aprovação: \_\_\_\_\_

\_\_\_\_\_  
Profº. Dr. Adriano Marteleto Godinho (Orientador)

\_\_\_\_\_  
Profª. Ma. Juliana Fernandes Moreira (Examinadora)

\_\_\_\_\_  
Profª. Ma. Ana Carolina Monteiro Lins de Albuquerque e Souto (Examinadora)

## **AGRADECIMENTOS**

Nessas breves palavras, devo agradecer primeiramente a Deus por nunca ter saído do meu lado, por me iluminar durante toda a minha vida, por me guiar durante toda essa trajetória acadêmica.

Agradeço especialmente à minha mãe que, sempre com muito amor e zelo, dedicou toda sua vida para minha formação pessoal e acadêmica. Agradeço pela paciência e sabedoria para lidar comigo diariamente, pois sem fraquejar, nem enlouquecer, carregou do meu lado todas as minhas cruzes.

Agradeço ao meu pai que sempre acreditou no meu potencial e esteve do meu lado me incentivando a ir sempre mais longe. Agradeço por sempre me proteger, com seu jeito especial, de tudo e de todos, por não permitir que nada, nem ninguém ousasse me fazer mal.

Os meus sinceros agradecimentos ao meu professor e orientador, Adriano Godinho, que confiou e acreditou no meu trabalho, e me auxiliou verdadeiramente na construção desse estudo (e da minha paixão pela matéria) com muita paciência e disposição; um verdadeiro exemplo de educador e ser humano.

Agradeço a todos os meus colegas de dentro e de fora da universidade, por todo companheirismo, alegrias, conquistas e tantas outras contribuições para a construção da minha felicidade e sucesso.

Não posso deixar de agradecer ao meu namorado e verdadeiro companheiro, João Pedro, que mesmo com nossa singela história, esteve a todo tempo do meu lado, com palavras de incentivo, com muita apoio e paciência.

## RESUMO

Com suporte na perspectiva do Direito Civil Constitucional humanizado, em que os institutos e as tutelas do direito privado devem se estender para além de situações patrimonialistas, tornando, com isso, o ser humano centro referencial do ordenamento. A edição da Constituição de 1988, que instaurou uma nova ordem jurídica, fez com que os conceitos e os princípios civilistas passassem a ser reconstruídos à luz dessa nova visão constitucional humanizada. Diante da utilização intensa de tecnologias de informação, que visam a coleta, armazenamento e processamento de dados, violações à privacidade e à intimidade se intensificaram, principalmente quando utilizadas sobre dados pessoais. A utilização indevida da referida tecnologia pode revelar dados da vida privada, que muitas vezes ocorre sem o consentimento do titular, constituindo uma violação direta à privacidade dos sujeitos de direito. Portanto, faz-se necessária a regulamentação devida de tais instrumentos com fulcro na proteção dos dados pessoais dos brasileiros, pois os avanços tecnológicos e utilização de banco de dados não irão findar ou retroceder. Para isto, vale tomar como base os modelos regulatórios de proteção de dados já existentes em países estrangeiros. O presente trabalho conta com uma pesquisa bibliográfica de diversos estudos de literatura nacional e estrangeira, para embasar o entendimento quanto o direito à privacidade e a dignidade da pessoa humana. Verifica-se que a privacidade se encontra em estado acuado diante das tecnologias da informação e, portanto, o objetivo deste trabalho é cooperar para que a comunidade interprete a melhor aplicação do instituto da privacidade, mesmo na presença das mais diversas maneiras de violação e ameaça à privacidade e à intimidade. Faz-se relevante a instauração de medidas administrativas e legislativas para garantir, efetivamente, o referido direito fundamental, regulamentando a utilização das tecnologias, bem como conscientização social dos riscos que os dados pessoais estão expostos.

**Palavras-chave:** Privacidade. Intimidade. Humanização. Tecnologia da informação. Dados pessoais.

## SUMÁRIO

<b>1 INTRODUÇÃO.....</b>	<b>8</b>
<b>2 A PRIVACIDADE HUMANIZADA NA PERSPECTIVA DO DIREITO CIVIL-CONSTITUCIONAL.....</b>	<b>12</b>
2.1 A PERSONALIDADE E O SUJEITO DE DIREITO: A PESSOA COMO CENTRO MAIOR DO ORDENAMENTO JURÍDICO.....	12
2.2 OS DIREITOS DA PERSONALIDADE SOB A PERSPECTIVA HUMANIZADA.....	15
2.3 CONCEITUAÇÃO DO DIREITO À PRIVACIDADE.....	18
2.4 TEORIA DAS ESFERAS – A DISTINÇÃO ENTRE A PRIVACIDADE E A INTIMIDADE.....	22
<b>3 SOCIEDADE DA INFORMAÇÃO: DADOS PESSOAS E TECNOLOGIAS DIANTE DO DIREITO À PRIVACIDADE.....</b>	<b>26</b>
3.1 SOCIEDADE DA INFORMAÇÃO, DADOS PESSOAIS E BANCO DE DADOS.....	26
3.2 TÉCNICAS DE PROCESSAMENTO E TRATAMENTO DE DADOS.....	32
<b>4 MEIOS DE TUTELA E DE PROTEÇÃO DOS DADOS PESSOAIS.....</b>	<b>38</b>
4.1 A CONFLUÊNCIA INTERNACIONAL NA POLÍTICA DE PROTEÇÃO DE DADOS.....	38
4.2 MODELOS REFERÊNCIAS DE REGULAÇÃO E PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO INTERNACIONAL.....	43
4.2.1 Sistema Regulatório Europeu.....	44
4.2.2 Sistema Regulatório Norte-americano.....	46

<b>4.2.3 Sistema Regulatório Uruguaio.....</b>	<b>48</b>
<b>5 PERSPECTIVAS PARA INSTITUIÇÃO DE UM SISTEMA REGULATÓRIO BRASILEIRO DE DADOS PESSOAIS.....</b>	<b>52</b>
5.1 LEGISLAÇÃO NACIONAL DE PROTEÇÃO À INTIMIDADE COM FULCRO NAS INFORMAÇÕES PESSOAIS.....	53
5.2 PROJETOS DE LEIS QUE VERSAM ESPECIFICAMENTE SOBRE PROTEÇÃO DE DADOS PESSOAIS.....	57
5.2.1 Projeto de Lei nº 5.276/2016.....	57
5.2.2 Projeto de Lei nº 330/2013.....	59
<b>6 CONCLUSÃO.....</b>	<b>64</b>
<b>REFERÊNCIAS.....</b>	<b>67</b>



## 1 INTRODUÇÃO

O presente Trabalho de Conclusão de Curso está inserido no ramo do Direito Civil-Constitucional, referindo-se particularmente ao direito à privacidade – que está incluído no rol dos direitos fundamentais constitucionais, bem como previsto no Código Civil de 2002 como um dos direitos da personalidade – com fulcro na proteção dos dados pessoais, especialmente aqueles que estão em meios informatizados.

Portanto, é possível afirmar que neste estudo são utilizados critérios de verificação de novos fenômenos tecnológicos impostos a nossa sociedade e a forma como estes apresentam grave interferência – muitas vezes indevida – na privacidade e intimidade alheias.

Sabe-se que por se tratar de um tema inovador e em constante modificação, os estudos realizados sobre a violação da privacidade devido aos inúmeros fenômenos tecnológicos não são tão vastos ou acessíveis, principalmente quanto ao ordenamento brasileiro. Entretanto, é cristalino que, diante da globalização, o nosso país não está distante da realidade da organização e administração de dados pessoais em bancos de dados informatizados, e, por isso, o Direito e a legislação também não poderão se manter indiferentes

Deste modo, o mero conhecimento legislativo não se faz suficiente para a compreensão da problemática analisada no presente estudo, pois é fundamental a realização de pesquisa aprofundada quanto à extensão do direito à privacidade e todas as garantias que são concedidas por ele, juntamente com todas as ameaças e violações que o Direito poderá enfrentar.

A pertinência do presente trabalho se demonstra, principalmente, na pesquisa em território nacional, para que o acervo da literatura sobre o tema seja aumentado, melhor compreendido e divulgado para a comunidade. Com isso, será possível facilitar a consolidação de um posicionamento do ordenamento jurídico quanto às ameaças e violações ao direito à privacidade.

Isto porque, as ameaças e lesões à intimidade e à privacidade permanecem em estado latente em nossa legislação, pois, embora exista a violação direta a este direito da personalidade, a sociedade não se dá conta de tal ocorrência ou, ainda que saiba, não busca os meios de tutela devidos.

Diante dessa nova perspectiva de Direito Civil constitucionalizado e humanizado, o direito à privacidade está intrinsecamente ligado aos direitos fundamentais e ao princípio da dignidade da pessoa humana. Logo, além de facilitar a compreensão das diversas faces do direito à privacidade, principalmente à luz da dignidade da pessoa humana, o presente estudo demonstra-se fundamental para demonstrar possíveis violações e lesões para que o ordenamento brasileiro se molde às modificações inauguradas por bancos de dados pessoais entre outras tecnologias da informação, que serão delineadas no desenvolvimento deste trabalho.

O avanço da informática suscitou inúmeros problemas para o Direito, em virtude da globalização e universalização da comunicação eletrônica. O acesso a informações e dados pessoais revelam dados da vida privada, o que, por muitas vezes, ocorre sem o consentimento do titular, constituindo, portanto, uma intrusão ilícita na vida pessoal do indivíduo, ou seja, uma violação imediata ao direito à privacidade. Por esta razão, será também de suma importância analisar o Marco Civil da Internet, bem como outros Projetos de Lei que tramitam no Congresso Nacional, como forma de compreender os institutos jurídicos já existentes e que estão para entrar em vigor, que objetivam proteger a privacidade e a intimidade.

Este estudo tem como objetivo o aprofundamento na percepção de boa parte das violações ou ameaças ao direito à privacidade que podem ocorrer por força da má administração ou processamento indevido de dados pessoais. Com isso, buscar-se-á a compreensão da melhor utilização destas ferramentas e demonstrar uma regulamentação devida para estes instrumentos.

Os avanços tecnológicos e a utilização de bancos de dados dificilmente irão cessar ou regredir, pois a tendência é a sua evolução; conseqüentemente, as mais severas violações e ameaças à privacidade podem ser provocadas. Portanto, o presente trabalho, além de propiciar melhor entendimento das diversas facetas da privacidade e dignidade da pessoa humana, irá analisar as legislações estrangeiras sobre o tema, os meios de tutela existentes em nosso Estado.

A relevância do presente trabalho para comunidade acadêmica, bem como para a sociedade, é a de apresentar as ameaças e lesões que estão latentes na vida de todos, tornando possível uma regulamentação e melhor fiscalização das práticas violadoras da

privacidade. Inclusive, é possível afirmar que será justificado a necessidade de alteração da legislação nacional, diante das legislações internacionais já existentes.

Neste sentido, faz-se mister ressaltar a Convenção 108 (UNIÃO EUROPEIA, 1981), assinada pelos Estados membros do Conselho da Europa<sup>1</sup>, que visava a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal. Esta convenção em seu texto demonstra que os Estados membros buscarão a proteção dos direitos e liberdades fundamentais de todos os europeus em respeito à vida privada, diante do fluxo crescente dentre fronteiras de dados pessoais suscetíveis de tratamento automatizado.

Assim, a supracitada Convenção pode facilmente servir de referência para o nosso ordenamento de forma que garanta uma proteção satisfatória ao direito à privacidade dos brasileiros relativos às lesões feitas pelo processamento e armazenamento de dados pessoais. A intenção deste trabalho, deste modo, é levantar legislações esparsas da comunidade internacional e demonstrar a sua relevância para o ordenamento brasileiro, por meio do método comparativo.

O tipo de pesquisa a ser utilizado neste Trabalho de Conclusão de Curso é a pesquisa exploratória, que será realizada através de estudos de literaturas nacionais e internacionais, moldando as problemáticas nacionais às legislações estrangeiras. Além disso, será efetuada uma pesquisa bibliográfica em que abarcará coletânea de textos e artigos brasileiros e estrangeiros, que contenha o tema do direito à privacidade e a dignidade da pessoa humana, de forma conceitual e genérica, bem como tais institutos voltados para à proteção de dados pessoais.

Ainda, a abordagem a ser realizada é a hipotética-dedutiva, pois diante da ínfima quantidade de estudos acadêmicos voltados ao objeto da presente pesquisa, o embasamento do presente trabalho será hipotético e, em seguida, dedutivamente será verificado o objetivo final da pesquisa, qual seja, compreender o direito à privacidade diante do processamento de dados pessoais e demonstrar possíveis meios de tutela. O procedimento científico a ser utilizado será experimental comparativo, visto que a pesquisa se baseia em situações a serem verificadas à luz do instituto da privacidade,

---

<sup>1</sup> O Conselho Europeu é o mais alto órgão do bloco econômico da União Europeia, composto pelos chefes de Estado ou de Governo dos estados membros juntamente com o Presidente da Comissão europeia.

comparando os casos estrangeiros para que o estudo possa ser aplicado em território nacional.

Quanto ao desenvolvimento do presente trabalho, este contém quatro capítulos, quais sejam o primeiro demonstrará a nova perspectiva do Direito Civil- Constitucional Humanizado, apresentando os institutos da personalidade, dos direitos da personalidade, para que ao final, conclua-o conceituando o enfoque do presente trabalho: o direito à privacidade.

Em seguida, serão tratados conceitos técnicos informáticos e informacionais, ou seja, tais institutos jurídicos serão analisados à luz de alguns mecanismos eletrônicos. Inicialmente, será conceituada a nova sociedade da informação, demonstrando os conceitos de dados pessoais, banco dados, entre outros. Concluindo o capítulo demonstrando a forma que estes mecanismos podem violar o direito à privacidade e a intimidade.

O terceiro capítulo, por sua vez, apresentará os meios de proteção e tutela dos dados pessoais no âmbito internacional, como forma de tomar referência de tais legislações para o ordenamento jurídico brasileiro. Neste capítulo, serão delineados, brevemente, os modelos europeu, norte-americano e uruguaio.

O último capítulo volta-se a demonstrar as legislações nacionais existentes passíveis de proteção ao direito à privacidade e aos dados pessoais dos cidadãos brasileiros. Em seguida, serão tratados alguns projetos de leis, em trâmite, que buscam a construção de uma Norma Geral de Proteção de Dados Pessoais no Brasil. Já na conclusão, serão reapresentados os pontos principais e fundamentais do trabalho de conclusão de curso, reafirmando a pertinência da temática aqui escolhida, bem como demonstrando a necessidade da referida Norma, como forma urgente de proteção à privacidade e intimidade.

## **2 A PRIVACIDADE HUMANIZADA NA PERSPECTIVA DO DIREITO CIVIL-CONSTITUCIONAL**

O presente capítulo tem por objetivo demonstrar a nova perspectiva do Direito Civil humanizado à luz das regras e princípios constitucionais. Isto porque, o direito contemporâneo exige uma releitura dos conceitos e institutos jurídicos a partir de valores máximos empregados pela Carta Magna.

Desenvolve-se nesse primeiro capítulo uma diferenciação entre o sujeito de direito e a personalidade, em si. Essa distinção demonstra-se fundamental para comprovar a supracitada intenção deste capítulo, ou seja, esclarecer os institutos e conceitos jurídicos apoiados numa perspectiva humanizada. Em seguida, volta-se para os direitos à personalidade, conceituando-os através de sua forma humanizada. Por fim, aprofunda-se para o enfoque do presente estudo: o direito à privacidade, trazendo seus conceitos sociológicos, doutrinários e jurídicos.

### **2.1 A PERSONALIDADE E O SUJEITO DE DIREITO: A PESSOA COMO EPICENTRO MAIOR DO ORDENAMENTO JURÍDICO**

O Código Civil de 2002, que já fora editado à luz da Constituição Humana de 1988, dispõe em seus primeiros dispositivos a consagração de todos os seres humanos como pessoas, que para o Direito esse conceito se distingue do social comum. Deste modo, enquanto no conhecimento comum o vocábulo pessoa é sinônimo de ser humano, para o Direito ser pessoa é a possibilidade de ser sujeito de direito, titular de direitos, ou seja, dando-lhe a possibilidade de assumir a titularidade de direitos existenciais e patrimoniais e de integrar o polo de uma relação jurídica.

Contudo, esse entendimento deve ser estendido, no sentido de que o sujeito de direito, dotado de personalidade civil, não pode ser conceituado tão somente como a possibilidade de se atuar em cenários jurídicos, ou seja, para ser considerado pessoa não é necessário apenas ter direitos, mas ter a possibilidade de vir a ter direitos – perceba-se que há uma conotação futura, pois, a possibilidade de ter direitos (passado e presente) distingue-se da possibilidade de vir a ter direitos (futuro).

Com a edição da Carta Magna, foi instaurada uma nova ordem jurídica no Brasil, a qual instituiu novos institutos valorativos e novos princípios norteadores e, com isso, essa normativa constitucional passou a incidir nas relações particulares e intersubjetivas.

Portanto, os regramentos e influências sociais do direito civil passou a ser vislumbrado a partir de novos valores, pois os conceitos do Direito Civil passaram a ser reconstruídos à luz da nova visão constitucional.

A expansão do Direito Civil, no sentido de se revisar os seus conceitos e paradigmas, deve ser compreendido de tal maneira que a sua tutela se estenda para além das situações patrimoniais. Isto porque, a pessoa passou a ser o centro de referência do ordenamento, e não tão somente a pecúnia. Com essa nova perspectiva constitucional do Direito Civil, é necessária a superação do entendimento de que a personalidade se esgota na aptidão do sujeito ser titular de direito, ou seja, a personalidade não deve ser compreendida como sinônimo de capacidade.

Na verdade, a personalidade deve ser interpretada por duas faces do mesmo conceito. A primeira face, como já dito, é a possibilidade de o sujeito ser titular de direitos e obrigações – e, neste caso, essa possibilidade é conferida não apenas as pessoas naturais, mas também às pessoas jurídicas. Por isso, jamais a personalidade poderia se restringir a esta faceta, pois o direito acabaria por colocar no mesmo plano valorativo a tutela da pessoa natural e aquela conferida às pessoas jurídicas, o que seria uma atrocidade jurídica.

Já a segunda face da personalidade é o reconhecimento deste instituto como valor ético, que emana do princípio da dignidade da pessoa humana, ou seja, a personalidade não deve se resumir a titularidade de direitos de forma abstrata, mas deve ser entendida como o reconhecimento de direitos que são exclusivos da pessoa humana, que só alcançam a pessoa através do princípio da dignidade da pessoa humana. Portanto, a personalidade é a expressão da própria existência humana.

Deste modo, deve ficar cristalino que a personalidade não é um objeto do sujeito de direito, na verdade, transcende-o, pois não se exaure em uma categoria de direito subjetivo. Os direitos da personalidade são consequências de uma compreensão extensiva da pessoa humana como valor, que, por ser dotada de atributos inerentes, exclusivos e indispensáveis, demanda uma tutela privilegiada.

A humanização do Direito Civil Constitucionalizado faz com que os atos de vontade (atos da vida civil) dos sujeitos de direito não possuam tanta relevância e centralidade para o ordenamento jurídico frente aos bens jurídicos intrínsecos da pessoa natural. Isto porque, tais atos perdem seu valor diante do alto grau de proteção que é dado à pessoa humana, ou seja, essa nova perspectiva faz com que o ser humano seja o centro

nuclear de todo o Direito, isto é, a razão da existência de um ordenamento jurídico deve ser voltada à proteção e promoção do desenvolvimento das pessoas.

É neste sentido que se faz fundamental destacar as lições de Gustavo Tepedino (2013, p. 50):

Portanto, as situações existenciais, ou seja, aquelas que apresentam em seu núcleo interesse diretamente voltados à proteção da personalidade, ocupam no ordenamento jurídico uma posição de primazia frente às demais situações cujos interesses diretos são de cunho patrimonial. Mas podermos ir ainda além, radicalizando o valor que a pessoa ocupa no Direito, a fim de afirmarmos que a própria tutela conferida pelo ordenamento às ditas situações patrimoniais tem como finalidade última realização do homem, razão pela qual tais situações são funcionalizadas, ou seja, compreendidas como instrumento ou suporte ao livre desenvolvimento da pessoa, que constitui, portanto, a tarefa do Direito Civil atual.

Com isso, diante de todo esse reconhecimento de que a pessoa humana é o centro do ordenamento jurídico, a dicotomia entre direito público e privado acaba por perder tanta relevância e espaço na doutrina jurídica. Inclusive, é fácil de se afirmar que o Direito Civil Constitucionalizado é considerado como um fenômeno de publicização do direito privado, ou seja, há uma superação da dicotomia retrocitada.

A tutela da pessoa extrapola o entendimento limitado de relações entre Estado e sujeito, estendendo-se de maneira a alcançar toda e qualquer relação, inclusive as relações entre particulares. Percebe-se, portanto, que não é função privativa do Estado proteger a pessoa, mas, na verdade, de toda sociedade e seus particulares em qualquer esfera de atuação.

Voltando-se para o ordenamento brasileiro, tem-se a Constituição de 1988 que adotou como fundamento da República, em seu artigo 1º, inciso III, a dignidade da pessoa humana. O referido princípio deve orientar toda e qualquer atividade legislativa, seja ela de âmbito público ou privado. Logo, todos os institutos civilistas devem ser interpretados e aplicados em conformidade com a Carta Magna e seus princípios.

A dignidade da pessoa humana como valor norteador do Direito Civil faz com que as situações jurídicas extrapatrimoniais superem as patrimoniais, no sentido de valoração jurídica. Ora, toda a legislação civilista deve, portanto, ultrapassar das situações patológicas dos direitos da personalidade, ou seja, não deve estar apenas voltada no dever de reparação – uma normatização preocupada em operações de indenização –, pois, o

direito civil deve coordenar as atividades privadas como forma de concretização do fundamento principal da República Brasileira, a dignidade da pessoa humana.

## 2.2 OS DIREITOS DA PERSONALIDADE SOB A PERSPECTIVA HUMANIZADA

A definição dos direitos da personalidade é vista de inúmeras maneiras, sob diversos olhares da doutrina e, por esta razão, será buscado o conceito que mais se adequa à ótica humanizada civil-constitucional do ordenamento brasileiro. Inicialmente, é possível afirmar que os direitos da personalidade são direitos inatos da pessoa humana, no qual caberá ao Estado apenas o seu reconhecimento e positividade em plano legislativo – percebe-se a existência de um cunho obrigatório de proteção de tais direitos por parte do Estado.

Neste diapasão, Marcelo dos Santos (2014, p.7) reafirma os ideais de Bittar de forma bastante esclarecedora:

Sob o olhar de Bittar, considera-se como da personalidade os direitos reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previsto no ordenamento jurídico exatamente para a defesa de valores inatos no homem, como a vida, a higidez física, a intimidade, a honra, a intelectualidade e outros tantos.

Através desta concepção é que se percebe que a perspectiva humanizada do Direito Civil faz com que o ordenamento jurídico abandone de forma gradativa a sua rigidez e seu formalismo para ser conduzido por meio de valores maiores. Inclusive, é possível afirmar que esses ideais e valores no Direito Civil se deu através de seu processo de constitucionalização e humanização.

Ante a grandiosidade do ser humano e seus valores para o ordenamento jurídico, surge a denominada Cláusula Geral da Personalidade, que nasceu através da constitucionalização da proteção da personalidade, à luz da dignidade da pessoa humana. A referida cláusula é utilizada nas situações em que um direito da personalidade é posto em discussão, a fim de que a decisão a ser tomada seja dada com prioridade à pessoa humana.

Quanto à suposta classificação dos direitos da personalidade, a doutrina se divide em dois entendimentos. O primeiro aduz que existem diversos direitos, limitados e positivados em legislação, nos quais se transformam em bens jurídicos relevantes para a vida humana. Entretanto, o posicionamento que prevalece, após a humanização do Direito Civil, entende que os direitos da personalidade não se limitam a um simples rol editado



pelo legislador. Na verdade, esse rol é meramente exemplificativo, pois o ser humano deve ter seu corpo e intelecto protegido em sua integralidade à luz da dignidade da pessoa humana.

Trata-se de uma tutela geral da personalidade, a qual é protegida através da Cláusula Geral da Personalidade, que deve ser reconhecida através da constitucionalização do direito civil. Essa amplitude protecionista da referida cláusula para com os direitos da personalidade emerge de forma a resguardar a dignidade da pessoa humana, que se demonstrou cada vez mais fundamental, principalmente em razão dos avanços científicos e tecnológicos da contemporaneidade.

Importante demonstrar o entendimento de Gustavo Tepedino (2013, p.61), quanto à proteção dos direitos da personalidade:

Um eventual tratamento de diversas hipóteses particulares de direitos da personalidade não deve induzir ao pensamento de que a proteção humana seja fragmentada. Pelo contrário, pelo estudo apartado das especificidades de cada grupo de casos é possível chegar a uma tutela específica e eficaz para cada caso.

A existência de uma cláusula geral da personalidade não faz confundir cada particularidade dos direitos da personalidade, nem a existência de diversos direitos da personalidade faz-se pensar que a proteção destes deve ser feita de forma apartada. Na verdade, a diversidade de tratamento entre os direitos da personalidade faz com que cada um apresente suas adversidades específicas, mas que todos tenham um referencial único que é a dignidade da pessoa humana.

É neste sentido que é possível afirmar que o legislador civilista brasileiro não teve a intenção de trazer no Código Civil de 2002 um rol exaustivo de direitos da personalidade, na verdade, trata-se de verdadeiros direitos principiológicos a serem observados por todo ordenamento jurídico, pois estão em conformidade com a atual ordem humanizada.

Deste modo, passa-se para uma breve análise dos dispositivos do supracitado Código, que versem sobre os direitos da personalidade. O artigo 11 cuidou de tratar das características do direito da personalidade, quais sejam: intransmissibilidade, irrenunciabilidade e impossibilidade de limitação voluntária do seu exercício – devendo-se atentar que além destas, a doutrina cuidou de trazer outras características aos direitos da personalidade.

A intransmissibilidade significa que nenhum direito da personalidade pode ser cedido ou sucedido, pois trata-se de uma verdadeira expressão da personalidade do titular do direito, impedindo a aquisição por terceiro. Já a irrenunciabilidade determina que, por serem direitos inerentes da pessoa, ou seja, por nascerem junto ao ser humano, jamais poderão ser renunciados, nem sequer passíveis de limitação para o exercício dos referidos direitos voluntariamente.

A doutrina, ainda, afirma que são direitos imprescritíveis, ou seja, não é possível a sua extinção pelo decurso do tempo, pela demora de defendê-lo em juízo ou pelo não uso. Entretanto, é possível existir prazo pleitear compensação pecuniária pelo dano extrapatrimonial decorrente da lesão ou ameaça ao direito.

Portanto, os direitos da personalidade são direitos extrapatrimoniais, ou seja, não compreendem valores redutíveis a pecúnia, pois não possuem conteúdo patrimonial. Vale ressaltar que é admitido que os direitos da personalidade tenham repercussão pecuniária no sentido de se haver uma compensação econômica para o lesado.

Tais características existem com o objetivo de deixar claro a distinção dos direitos da personalidade de todos os demais direitos subjetivos. Até porque, como já dito, não é possível considerar o direito da personalidade como direito subjetivo, pois senão estaria reduzindo a personalidade a uma categoria de direito pecuniário e voltada à circulação de mercadorias, fugindo da proteção à pessoa humana.

O art. 11 do Código Civil dispõe o seguinte: “Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária” (BRASIL, 2002). O primeiro trecho do dispositivo poderia levar a conclusão contrária a todas as regras já fundamentadas aqui, entretanto, esse texto deve ser interpretado de forma ponderada, de modo que a lei que excetuar tais características, ainda assim, deve respeito às garantias constitucionais.

Ultrapassadas as características de todos os direitos da personalidade, convém traçar, brevemente, cada um deles. Entre os artigos 13 a 15, do Código Civil, há o direito à integridade psicofísica – diz-se integridade psicofísica, pois no Enunciado nº 6, que foi aprovado na I Jornada de Direito Civil, dispõe: “a expressão “exigência médica” contida no art. 13 refere-se tanto ao bem-estar físico quanto ao bem-estar psíquico do disponente” (I JORNADA DE DIREITO CIVIL, 2002).

Importante trazer esse enunciado, pois, embora alguns autores prefiram tratar a integridade física separada da integridade psíquica, hodiernamente já estão por superadas as concepções que tratam o estado psicológico separado do estado físico – isto porque seria mais uma maneira de fragmentar a tutela da própria condição humana, ou seja, dos direitos da personalidade.

Os artigos 16 a 19 do supracitado diploma legal regula o direito ao nome, em que reconhece o direito universal ao nome (composto por prenome e sobrenome). Tem-se como obrigatório, por meio de lei, em todo nascimento, levar a criança em registro civil para que lhe seja dado um nome. Ademais, o direito ao nome é estendido ao pseudônimo, pois a proteção dada por estes dispositivos não é concedida tão somente ao nome em si, mas a identidade pessoal do ser humano – portanto, abrange também ao pseudônimo.

O art. 20, por sua vez, versa sobre o direito à imagem, protegendo-a com certas ressalvas, pois a divulgação da imagem só será ilícita caso macule a honra, a boa-fama ou quando tenha fins lucrativos – diferentemente do Código Civil Português que regulamento que a mera divulgação de retrato pessoal está vinculado ao consentimento prévio, salvo notoriedade de cargo ou necessidade pública.

Por fim, o art. 21 regulamenta o direito à privacidade, que tem por objetivo proteger o resguardo pessoal, dispondo que a vida privada da pessoa natural é inviolável. A proteção da privacidade é um tema bastante delicado diante da contemporaneidade, pois é claro que vivemos diante de ofensas em estado potencial. Isto porque, o crescimento súbito do desenvolvimento tecnológico, bem como a dificuldade que o legislador se depara para acompanhar o referido desenvolvimento, não viabiliza uma proteção efetiva da privacidade.

### 2.3 CONCEITUAÇÃO DO DIREITO À PRIVACIDADE

Na obra “1984” de George Orwell a privacidade é um dos bens mais valiosos e caros para o indivíduo, pois, uma vez destituído da privacidade, o ser humano viola a sua própria personalidade. A referida obra demonstra uma sociedade dominada por um governo totalitário em que tudo era feito pela coletividade, ainda que cada sujeito vivesse solitário.

Na sociedade representada por Orwell, todos estavam sob vigilância do Grande Irmão – como se denominava o governo – e a privacidade era algo tão valioso para os

indivíduos que podia ser considerado como intangível. Neste conto, os sujeitos tinham aniquilada a sua privacidade, sendo lesionada diretamente a sua dignidade da pessoa humana.

Não há dúvidas do caráter vanguardista da referida obra, sendo incontáveis as semelhanças daquela ficção com a atual realidade. A privacidade, como já demonstrado desde o início desde trabalho, é inafastável da pessoa humana, por ser considerado direito da personalidade cujo seu núcleo corresponde diretamente à dignidade da pessoa humana.

A privacidade é considerada um direito fundamental dentre os direitos da personalidade, e a sua proteção se demonstra cada vez mais essencial e a sua efetivação cada vez mais distante, conforme será demonstrado durante todo o desenvolvimento do presente trabalho. Neste diapasão, inicialmente, é necessário compreender a privacidade e seus conceitos doutrinários.

Em termos mais sociológicos, a privacidade pode ser considerada um estado psicológico de “estar afastado dos demais”, ou também pode ser conceituado como o poder que o sujeito tem de controlar toda informação sobre si mesmo, ou seja, a possibilidade de controlar a circulação de informações pessoais. Neste mesmo sentido, afirma-se que a privacidade concede ao sujeito um espaço reservado e inviolável para que explore seu íntimo livremente, sem nenhuma máscara imposta pela sociedade, ou seja, exercer de forma plena seu direito à autodeterminação.

Sobre o tema Vieira (2007, p. 51-52) afirma:

O homem, ao contrário dos outros animais, detém a prerrogativa de realizar a denominada torção radial, ou seja, abandonar o mundo externo e voltar-se para dentro de si, ocupando-se apenas de si próprio e não do outro. Essa faculdade de ensimermar-se implica dois poderes: o de desatender o mundo externo e o de desenvolver com liberdade as próprias ideias. Daí a necessidade de proteção à privacidade, como único meio de se garantir ao indivíduo a possibilidade de ensimesmamento e, desta forma, conferir-lhe um espaço livre de ingerências e de intervenções advindas de censura externa.

Existe uma íntima relação entre a privacidade e a liberdade, pois deve ser garantido ao sujeito a liberdade de deixar de representar os papéis que lhe são impostos pela sociedade, deve ser garantida a liberdade de auto avaliação e, por fim, a liberdade de comunicação de informações que o sujeito escolhe ou não compartilhar com todos. Há uma relação intrínseca de proteção, dependendo a existência da privacidade da liberdade,

pois o controle de pensamentos, a censura, a intromissão na vida pessoal – condutas típicas de regimes totalitários – são destruidores da privacidade.

Perceba, portanto, a existência de uma relação de interdependência entre a privacidade e liberdade, pois o sujeito, ao exercer sua privacidade, estará exercendo sua liberdade, ou seja, a liberdade de expor ou não informações sobre si, revelando ou não dados de sua titularidade publicamente. Faz-se mister esclarecer que o direito à privacidade garante a quietude contra a curiosidade alheia, impedindo a exposição da vida particular, enquanto que o direito à liberdade dispõe ao indivíduo a escolha daquilo que pretende externar ou não.

Ultrapassados tais entendimentos, torna-se viável a conceituação da privacidade como a faculdade dada aos sujeitos de impedir a intromissão de alheios em sua vida particular e familiar, bem como obstar o acesso de informações sobre si e, por fim, impedir também a divulgação destas. Tatiana Vieira (2007, p.23), citando a obra *Direito à Privacidade na Internet*, de Marcelo Pereira, aponta: “o direito à intimidade seria (...) o poder das pessoas de controlar suas informações pessoais, as quais, ainda que não formem parte da vida privada das mesmas, possam revelar aspectos de sua personalidade”.

Perceba-se que o supracitado conceito demonstra que a proteção da privacidade é um tema bastante delicado, pois as ofensas a este direito da personalidade estão sempre em estado latente, devido ao crescimento abrupto das tecnologias e o avanço do mundo cibernético, que faz com que esse controle de informações pessoais fuja do controle do titular e este poder passe para terceiros.

No ordenamento brasileiro, a privacidade consiste no direito de toda pessoa, seja nacional ou estrangeira, residente ou não, de constranger terceiros a respeitarem a sua intimidade e a sua esfera privada, mas, além disso, é o direito de controlar as informações de caráter pessoal, possibilitando a resistência à intromissão indevida de pessoa alheia. Portanto, a privacidade é a garantia de controlar as informações pessoais e a prerrogativa de negar o acesso e a divulgação não autorizada de tais informações. Neste sentido, Tatiana Vieira (2007, p. 23) cita:

Tutela, portanto, o direito que se confere ao indivíduo de manter um afastamento confortável em relação ao mundo exterior, preservando esse distanciamento necessário ao exercício de sua autodeterminação. Tem, intrinsecamente, natureza negativa ao proteger o titular das intromissões de terceiros e, de outro lado, natureza positiva ao permitir que o próprio indivíduo controle o que deve ser conhecido e o que não

deve ser conhecido pelos demais, expressão da liberdade que lhe é ínsita.

Ainda que seja o mesmo direito, ou seja, o mesmo bem jurídico, a intimidade pode ser violada de duas maneiras, nas hipóteses em que a intromissão do terceiro à privacidade se consuma através do acesso não autorizado ou por meio de divulgação indevida de informações. Quanto ao acesso não autorizado, seria a situação em que a aquisição das informações particulares é ilegítima, enquanto que a divulgação é a hipótese em que a obtenção é autorizada, mas a revelação ulterior das informações é indevida.

Vale apresentar algumas categorias de classificação da privacidade, conforme a proteção que lhe é dada. A primeira delas é a privacidade física que, como o seu nome já apresenta, protege o corpo do sujeito contra procedimentos não autorizados, por exemplo, a realização de testes ou exames não autorizados.

A segunda categoria se refere à privacidade do domicílio, previsto no art. 5º, inciso XI, da Constituição da República, que protege o domicílio considerando-o como asilo inviolável, só podendo ser invadida nas hipóteses taxativas previstas neste dispositivo. Vale ressaltar que para fins de proteção constitucional o domicílio é considerado não só a residência, mas também escritórios e quartos de hotel.

Há também a privacidade das comunicações, disposta no art. 5º, inciso XII, da Constituição, que tem como garantia a inviolabilidade das correspondências, protegendo-a de particulares e do Poder Público, admitindo a sua violação apenas por meio de decisão judicial – jamais poderá ser decretada por agente público que não é magistrado, como, por exemplo, não poderá ser decretada a violação de correspondência em investigação de CPI, ou por delegado em inquérito policial. Além disso, vale ressaltar que o dispositivo ainda que não traga expressamente, a referida garantia se estende para correspondências eletrônicas.

A quarta espécie trata da privacidade decisional, também denominada de direito à autodeterminação, que é atributo inato a pessoa humana. A jurisprudência internacional reconheceu essa categoria em casos relativos ao uso ou não de anticoncepcional, a definição sexual, escolha de casar-se ou não, ou seja, é a garantia que o indivíduo determina de forma autônoma o seu destino.

A última categoria, que diz respeito ao foco do presente trabalho, consiste na privacidade informacional, que está voltada para a proteção das informações sobre o

titular do direito. Para esta categoria protege-se não apenas as informações relacionadas ao seu foro mais íntimo, mas também dados pessoais que possibilite a identificação do sujeito.

A jurisprudência alemã possui um caso em que há o reconhecimento desta categoria, que se refere a Lei do Censo em 1983. Esta lei determinou, para fins estatísticos, o recenseamento da população, ou seja, havia a coleta de dados sobre a moradia, a profissão, a renda e o domicílio das pessoas. A ordem legislativa previa a comparação dos dados levantados com os registros públicos já catalogados, bem como a possibilidade de transmissão dessas informações para os órgãos públicos.

Com isso, a Corte Alemã julgou como nulas todas as normas que possibilitavam a comparação e transmissão dos dados recolhidos para o Poder Público, reconhecendo a garantia à autodeterminação informativa dos alemães. Em outras palavras, o Poder Judiciário da Alemanha reconheceu o direito de cada indivíduo de controlar e proteger os dados pessoais sobre si, diante da tecnologia de dados e processamento da informação.

O direito à privacidade informacional já está previsto em inúmeras constituições estrangeiras, dentre elas a Constituição Portuguesa, porém a Constituição Brasileira não cuidou de editar um dispositivo que faça referência expressa a esta garantia. No entanto, realizando uma interpretação extensiva, tem-se uma suposta proteção à privacidade informacional no art. 5º, inciso XII, da Constituição, ao mencionar a proteção de dados genericamente.

#### 2.4 TEORIA DAS ESFERAS – A DISTINÇÃO ENTRE PRIVACIDADE E INTIMIDADE

A privacidade e a intimidade contam com os mesmos meios de tutela e a mesma proteção jurídica por nosso ordenamento, entretanto, ainda que bastante semelhantes, a doutrina sustenta que esses institutos são distintos, devido à fluidez existente nas esferas da vida particular. Isto porque, como já dito, o direito à privacidade é a garantia que o sujeito tem de impedir intromissão alheia em sua intimidade e vida privada – percebe-se que estes institutos estão inseridos dentro do direito à privacidade.

A vida privada é de certo modo mais abrangente, pois se refere à vida pessoal e familiar do sujeito, sendo possível haver conhecimento das informações daqueles que estão dentro da convivência do titular. Em outras palavras, trata-se de informações que

são, por escolha do indivíduo, compartilhadas às pessoas de sua confiança, e que estão distantes de um interesse público sobre elas.

Já a intimidade, que é mais restrita, reflete os pensamentos e emoções por se revelar o íntimo do indivíduo – ou melhor, trata-se de informações que o sujeito optou por guardar para si, por alcançar seu direito de discrição pessoal, tais como confidências, convicções e, até mesmo, dados pessoais. Portanto, infere-se que a intimidade reflete as informações que o sujeito guarda para si, sem compartilhar nem mesmo com seu círculo de confiança.

Importante apresentar o seguinte esclarecimento de Sidney Guerra (2004, p. 55) sobre o tema:

Verifica-se que a intimidade é algo a mais do que a vida privada, ou seja, a intimidade caracteriza-se por aquele espaço considerado pela pessoa como impenetrável, intransponível, indevassável e que, portanto, diz respeito única e exclusivamente a pessoa, como, por exemplo, recordações pessoais, memórias, diários, etc. Este espaço seria de tamanha importância que a pessoa não desejaria compartilhar com ninguém. São os segredos, as particularidades, as expectativas, enfim, seria o que vamos chamar de o “canto sagrado” que cada pessoa possui. Já a vida privada consiste naquelas particularidades que dizem respeito, por exemplo, à família, problemas envolvendo parentes próximos, saúde física e mental, etc. Seria então aquela esfera íntima de cada um, que vedasse a intromissão alheia. Entretanto, percebe-se que neste caso a pessoa poderia partilhá-la com as pessoas que bem lhe conviesse, sendo da família ou apenas um amigo próximo.

A doutrina alemã propôs a Teoria das Esferas, que busca demonstrar com maior clareza a distinção entre o privado, o íntimo e o secreto e, para tanto, fez-se uso da representação de três esferas concêntricas: *Privatsphäre*, *Intimsphäre* e *Geheimsphäre*. O primeiro círculo possui maior amplitude, pois representa a esfera privada do sujeito, compreendendo aspectos específicos da vida pessoal, mas que abrange o número considerável de relações interpessoais. Trata-se de informações nas quais o sujeito almeja excluir do conhecimento alheio, ou seja, de pessoas estranhas, como seus costumes e a sua imagem, por exemplo.

Já o segundo possui acesso mais restrito, compreendendo valores atinentes à esfera confidencial do sujeito e, portanto, o titular compartilha apenas com aqueles que possui relação mais íntima. Nesta circunferência encontra-se o sigilo domiciliar e profissional, dados íntimos, opção sexual e política, entre outros. O último círculo, por sua vez, é o menor de todos, onde se encontram as informações secretas ou sigilosas sobre



o sujeito, aquelas que não são compartilhadas ou, quando são, apenas para o número ínfimo de pessoas que são extremamente íntimas. Trata-se das informações como os sonhos, sentimentos, entre outros.

Ora, por meio da Teoria das Esferas, fica mais fácil de compreender a distinção entre intimidade e vida privada, podendo, inclusive, distinguir ambas do segredo. Deste modo, protege-se a vida privada por meio do direito que o titular possui de afastar do conhecimento público os acontecimentos de sua vida particular, mas que não se refere aos aspectos reservados de sua personalidade, enquanto que a intimidade se revela na prerrogativa de se excluir do domínio de terceiros as informações mais íntimas a respeito do indivíduo, atinentes à vida religiosa, por exemplo. Já os segredos são referências que o sujeito opta por não compartilhar com ninguém, geralmente.

Ainda que seja bastante dificultoso separar de forma objetiva essas esferas, pois não há fronteiras específicas que demarcam as circunferências, deve-se manter em mente que a menor das esferas – a esfera do segredo – deve ser inviolável de forma absoluta, de maneira que não pode ser atingida nem pelo Estado, nem por decisão judicial, nem por meio de lei, ou seja, não pode ser submetida por nenhuma ação do Poder Público. Ao passo que as informações contidas nas demais esferas, ainda que respeitadas e garantidas pelo ordenamento jurídico, não possui caráter absoluto, ou seja, é plenamente possível que o Poder Público, respeitadas as determinações legais, acessar essas esferas, desde que sejam garantidas a dignidade e a autodeterminação do indivíduo.

Inclusive, neste ponto específico de acesso do Poder Público a dados pessoais, demonstra-se relevante essa distinção entre vida privada e intimidade para fins de reparação por eventuais danos extrapatrimoniais. Isto porque, ainda que a vida privada e a intimidade sejam protegidas pelo mesmo instituto legal, a última deve receber uma proteção maior e mais efetiva, uma vez que abarca uma esfera mais íntima que aquela, de cunho ainda mais pessoal do titular. Logo, quanto mais interior a esfera atingida, ou seja, quanto mais íntima a informação acessada indevidamente ou divulgada ilegitimamente, maior deverá ser o valor indenizatório e a sanção imposta.

Em contrapartida da Teoria das Esferas existe a Teoria do Mosaico que também cabe ser apresentada no presente estudo. Fulgêncio Madrid, em sua obra “Derecho a la intimidad, informática y Estado de Derecho”, afirma que os dados pessoais são semelhantes a pequenas pedras que formam um mosaico, ou seja, vistas de forma

individual não representam grande relevância, porém, unindo-as, formam um conjunto relevante com grande significância. Com isso, o mosaico completo formaria a personalidade do indivíduo.

Para este autor a distinção entre esfera privada, intimidade e segredo é desimportante, pois, na verdade, a relevância se encontra no uso dos dados independentemente da circunferência destes. Portanto, trocando em miúdos a metáfora do mosaico, os dados que aparentemente se mostram inofensivos à violação do direito à privacidade, até mesmo aqueles presentes na maior esfera de todas, uma vez estruturados juntamente com outros dados, oferecem riscos tão graves quanto àqueles que estão na esfera do segredo. Portanto, para Fulgêncio, as informações particulares devem possuir a mesma proteção com a mesma intensidade, pouco importando a esfera em que se encontra o dado pessoal.

A Teoria do Mosaico e a Teoria das Esferas não podem ser refutadas entre si, elas não se excluem, pois, enquanto a última se demonstra relevante para a quantificação do valor reparatório, a primeira contribui para a compreensão da problemática da coleta e armazenamento de dados por entidades, sejam públicas ou privadas. Isto porque, os recursos tecnológicos permitem a conexão de inúmeras informações, ainda que pequenas, coletando inúmeros dados pessoais, construindo um perfil completo de forma indevida com grande velocidade.

Logo, tudo que foi narrado até o presente momento demonstra-se de grande relevância para situar o leitor nos institutos e conceitos jurídicos que serão abordados no presente trabalho, bem como o atual tratamento dado a estes diante da perspectiva humanizada, para que assim melhor compreenda a relevância de uma proteção efetiva aos dados pessoais, principalmente diante dos meios eletrônicos que estão postos em sociedade.

### **3 SOCIEDADE DA INFORMAÇÃO: DADOS PESSOAIS E TECNOLOGIAS DIANTE DO DIREITO À PRIVACIDADE**

Depois de discorrido sobre o Direito Civil humanizado e o direito à privacidade, segue-se rumo aos institutos e conceitos técnicos informáticos e informacionais. Trata-se, portanto, de uma análise desses institutos na conjuntura da sociedade da informação, com a utilização de bancos de dados e outros acervos tecnológicos para o mesmo fim.

Diante do desenvolvimento do poder computacional, que propicia o cruzamento de dados pessoais, bem como o monitoramento por vias eletrônicas de sujeitos e empresas, o direito à privacidade vê-se acuado. Como já dito na introdução do presente trabalho, o direito à privacidade, diante de tais avanços tecnológicos, não encontra forte apoio da doutrina brasileira, ou seja, não se vislumbram estudos aprofundados e reflexões jurídicas acuradas a respeito do tema.

Neste capítulo, serão conceituados os objetos e as técnicas que possibilitam a violação da privacidade, ou seja, serão tratados sobre os conceitos de sociedade da informação, dados pessoais, banco de dados, bem como a nova categoria de dados sensíveis. Por fim, serão versados sobre as técnicas utilizadas para processamento e armazenamento de dados.

#### **3.1 SOCIEDADE DA INFORMAÇÃO, DADOS PESSOAIS E BANCO DE DADOS**

Após a expansão da indústria da computação, a expressão “sociedade da informação” passou a ser empregada no início da década de 90, como forma de definir o abrupto uso da tecnologia da informação, que surgiu visando o avanço da economia, bem como a melhoria da prestação de serviços públicos e privados e da vida social.

Pode-se definir sociedade da informação como uma nova maneira de organização social, política e econômica que decorre de uma intensiva utilização da tecnologia para fins de armazenamento, produção e transmissão de informações. No entanto, a sociedade da informação, como forma de organização social, não pode ser confundida com a organização social conforme o modo de produção capitalista. Vieira (2007, p. 156) trata do tema da seguinte maneira:

Pode-se questionar que a expressão sociedade da informação define uma nova forma de organização social, pois, a rigor, o mundo continua organizado segundo o modo de produção capitalista. Há criação de um novo paradigma, tendo em vista o fato da informação, de per si, ter assumido maior relevância para a geração de riquezas, utilizando-se a tecnologia da informação enquanto

mecanismo facilitar de sua geração, processamento, transmissão e toda espécie de tratamento. Assim, embora a informação e a tecnologia da informação tenham assumido posição de destaque nesse novo cenário, configurando-se como verdadeiras mercadorias, não alteraram intrinsecamente as relações econômicas entre os diversos atores sociais, dinamizando apenas o já conhecido modo de produção capitalista.

Portanto, percebe-se que não há alteração intrínseca das relações econômicas entre os diversos agentes sociais da sociedade capitalista atual. Na verdade, houve uma otimização do modo de produção capitalista, através dessa nova posição de destaque conquistada pela informação e a tecnologia da informação.

Historicamente, pode-se alegar que, após a Revolução Industrial, tempo em que houve uma supervalorização da terra, vive-se atualmente em um enaltecimento da informação, ou seja, em uma verdadeira Revolução da Tecnologia da Informação<sup>2</sup>. O modelo capitalista atual tem como força primária a informação, que se coloca em posição decisiva para desenvolvimento da humanidade. Deste modelo, decorre a chamada tecnologia da informação, que é um mecanismo simplificador de produção, coleta, transmissão, processamento e armazenamento de dados – a referida tecnologia é causa de mudanças sociais a nível global.

A informação pode ser conceituada como um dado ou conjunto de dados, inserido em algum suporte, capaz de produzir alguma forma de conhecimento. Logo, é possível afirmar que a informação é imagem, som, documentos físicos e documentos eletrônicos. A sociedade hodierna vive de tal maneira que tudo depende da informação, ou seja, os dados ou conjuntos de dados consistem em uma das maiores riquezas da humanidade, pois são indispensáveis para o desempenho de qualquer atividade, essencial ou não essencial – saúde, lazer, política, educação, economia, entre outras.

Desta forma, os valores imateriais, os dados, as informações, o conhecimento científico, tudo está substituindo o capital e o trabalho, como fonte primária da formação e desenvolvimento sociológico. Portanto, a Revolução vivida nos dias atuais fez surgir a indústria e os serviços da informação – que engloba a fabricação de equipamentos e sistema de comunicação, bibliotecas e bancos de dados eletrônicos, mercados e serviços financeiros eletrônicos, entre tantos outros.

---

<sup>2</sup> Diferentemente de qualquer outra Revolução já vivida pela humanidade, que ocorria em uma área limitada do planeta, com expansão para demais áreas geografias de forma lenta e tardia, a Revolução da Tecnologia da Informação se espalha de forma exponencial e acelerada por todo o planeta em menos de duas décadas, impondo a todos e a tudo um padrão descontínuo e fluido nas bases da economia, da cultura, da política, entre outros.

Já os dados podem ser compreendidos como a informação em potencial, pois uma vez comunicado, recebido ou compreendido, poderá se transformar em uma informação por completo. Por exemplo, caso o dado se converta em palavras impressas, será compreendido de forma imediata pelo leitor, porém se o dado for apenas sinais que demandem estudo, ele permanecerá em um verdadeiro estado de “pré-informação”.

Especificamente, quanto aos dados pessoais, esses podem ser conceituados como fatos ou ações que se referem a circunstâncias de cunho pessoal acerca de um sujeito identificado ou identificável. É possível definir dados pessoais também como fatos, opiniões ou comunicações que se relacionam com o indivíduo, os quais seria razoável entender que ele consideraria íntimos e, portanto, desejaria escondê-los ou, pelo menos, restringir seu uso, circulação ou coleção.

Ao tratar dos dados pessoais, Catarina Sarmento e Castro (2005, p. 70-71), bem como Maria Eduarda Gonçalves (2003, p. 89), ambas citadas por Vieira (2007, p. 224-225), afirmam:

*Dado pessoal é o dado relacionado a um indivíduo identificado ou identificável, independentemente do suporte em que se encontre registrado (escrita, imagem som ou vídeo). Entende-se por identificado, o indivíduo que já é conhecido; e por identificável a pessoa que pode ser conhecida diretamente pelo próprio possuidor de seus dados, ou indiretamente através de recursos e meios à disposição de terceiros. Um exemplo de dado pessoal é o IP atribuído a um determinado computador quando este se conecta à rede. Apesar de essa informação não conduzir à identificação direta do internauta, tal identificação poderá ser conhecida a partir da interconexão com outros dados armazenados pelo provedor de acesso à internet, cybercafé, lan house, cyber office ou estabelecimento congênere. Assim, a identificação pode ser feita diretamente pelo próprio possuidor dos dados ou indiretamente por meio de terceiros. Entretanto, para não se resvalar ao absurdo de se classificar aleatoriamente qualquer informação relacionada com alguém como dado pessoal – o que implicaria a necessidade de adoção de procedimentos e de medidas especiais de proteção – devem-se considerar identificáveis apenas as pessoas físicas e jurídicas que possam ser conhecidas direta ou indiretamente, sem que seja necessário o dispêndio de tempo, custo ou esforço exagerado.*

Além deste conceito supracitado, de maneira mais prática, os dados pessoais são compreendidos como informações referentes ao sujeito que o tornam único em seu meio social, político e familiar. Deste modo, é possível classificar os dados pessoais em diversas espécies, quais sejam, as identificações numéricas que diferenciam o sujeito em sua sociedade – documento de identidade (Registro Geral, Cadastro de Pessoa Física, Carteira Nacional de Habilitação) –, que são identificações perante a comunidade jurídica.

É possível classificar, também, os dados pessoais como aqueles que distinguem o sujeito por meio de sua família, por sua idade, ou local que vive, que são os documentos de Certidão de Nascimento, Certidão de Casamento, Certidão de Óbito, entre outras – tais documentos também são de ordem jurídica, devido aos efeitos que produzem perante a sociedade. Há os dados de natureza meramente social ou educacional, como uma carteira de clube esportivo ou registro de matrícula, por exemplo. Portanto, percebe-se que um indivíduo carrega consigo inúmeras qualificações e identificações e, todas elas, devem gerar a devida proteção em relação ao uso não autorizado ou para fins ilícitos.

A Diretiva Europeia 95/46/CE (UNIÃO EUROPEIA, 1995) que versa sobre “à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados”, em seu art. 2º, alínea a, cuidou de conceituar dados pessoais da seguinte maneira:

Art. 2º. Para efeitos da presente diretiva, entende-se por:

- a) Dados pessoais, qualquer informação relativa a uma pessoa singular identificada ou identificável; é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos de identidade física, fisiológica, psíquica, econômica, cultural ou social.

Ainda, é plenamente possível que dados considerados pessoais se refiram a pessoas indeterminadas, que seria a hipótese de dados anônimos utilizados para fins estatísticos. Assim como os dados pessoais de sujeitos determinados ou determináveis, os dados pessoais de indivíduos anônimos merecem igual proteção e tratamento. Foi neste sentido que o julgado alemão sobre a Lei do Censo de 1983, já mencionado no primeiro capítulo deste trabalho, deu especial proteção aos dados coletados para o censo de pessoas indeterminadas.

Leonardo Martins (2005, p. 244-245) refere-se desta jurisprudência da seguinte maneira:

Uma eventual transmissão (entrega) dos dados que não sejam anônimos nem tenham sido processados estatisticamente – portanto, que sejam ainda pessoais – encerra problemas especiais. Os levantamentos de dados para fins estatísticos abrangem também dados individualizados de cada cidadão, que não são necessários para os fins estatísticos e que (...) servem apenas como auxiliares no processo de pesquisa. Todos esses dados podem até ser transmitidos a terceiros por força de expressa autorização legal, se na medida em que isso aconteça para o processamento estatístico por parte de outras autoridades, e para que as medidas prescritas em prol da proteção do direito e da personalidade, principalmente o sigilo estatístico e o princípio do anonimato sejam, tão logo possível, garantidas de maneira confiável, tanto na organização e procedimento

quanto nos órgãos estatísticos federais e estaduais. A transmissão a terceiros dos dados levantados para fins estatísticos, não anônimos nem processados estatisticamente para fins de execução administrativa, pode, ao contrário, intervir de forma inadmissível o direito de autodeterminação sobre a informação.

Ainda sobre dados pessoais, a Diretiva Europeia 95/46/CE (UNIÃO EUROPEIA, 1995), faz uso da expressão “tratamento de dados pessoais” quando quer versar acerca de operações que podem ser realizadas sobre os dados pessoais, seja por meio da informática ou não, desde que tenha como finalidade refinar a informação, de modo a torna-la mais útil ou valiosa. As formas de tratamento de dados pessoais podem ser: coleta, registro, organização, adaptação, conservação, recuperação, utilização, comunicação, difusão ou, até mesmo, a comparação, bloqueio, apagamento e destruição.

O referido tratamento tem um aspecto profundamente dinâmico, pois consiste no manejo da informação, de modo que são reelaborados dados para se obter conclusões específicas sobre um indivíduo ou um grupo de pessoas. Deste modo, para que os dados obtenham, de fato, sua finalidade precípua, eles devem ser armazenados e organizados em forma de banco de dados.

O banco de dados é definido, portanto, por um conjunto organizado e lógico de dados, como forma de facilitar a utilização e o acesso destes. Em outras palavras, o banco de dados é uma estrutura organizada, conforme critérios determinados, sobre dados pessoais, sejam de forma centralizada ou descentralizada, desde que organizados de forma funcional.

Os bancos de dados podem ser manuais ou automatizados. Os bancos de dados manuais são aqueles que são externados na forma de dossiê e fichários organizados, por exemplo. Já os bancos de dados automatizados são aqueles se encontram nos meios eletrônicos e tecnológicos. É inegável que a maior ameaça à privacidade se encontra na informatização do tratamento de dados pessoais, ou seja, nos bancos de dados automatizados, conforme será demonstrado em todo decorrer do presente trabalho. Logo, afirma Demócrito Reinaldo Filho (2005, p. 73), que as informações existentes em banco de dados informatizados:

[...] permitem que os registros neles contidos possam ser classificados segundo diferentes critérios e, desse modo, combinados entre si, num cruzamento que resulta na multiplicação e depuração da informação. Nisso se baseia o conceito de *inferential relational retrieval*, técnica que permite o recolhimento de dados dispersos e desconexos, sistematizando-os de forma a criar um perfil de comportamento de indivíduo qualquer. O cruzamento dos registros torna possível que os bancos de dados, formados geralmente por muitas bases e por inúmeros dados, multipliquem-se, o mesmo acontecendo em relação aos

critérios de classificação da informação. A formação dos bancos de dados está altamente facilitada. A antiga ideia de pessoas remexendo em fichas num escritório é a imagem de uma técnica há tempos abandonada. Com o auxílio da informática hoje é possível organizar sistematicamente qualquer dado, de forma simples e rápida. Ferramentas possibilitam aos usuários pesquisar quantias enormes de textos em busca de padrões e estruturas específicas. O texto então é convertido num banco de dados, cada arquivo em uma listagem de palavras, e para cada uma delas é criada uma lista de documentos onde cada palavra pode ser encontrada.

Diante de todos os meios eletrônicos que possibilitam o armazenamento, processamento e circulação de dados, surge uma nova categoria de dados que, caso utilizados, constituem uma ameaça colossal à personalidade e à privacidade do indivíduo, denominada de dados sensíveis. Portanto, é possível afirmar que a categoria dos dados sensíveis se refere a informações quanto à etnia, à opção sexual, à religião, à saúde, entre outras condições, do sujeito, que, se utilizados indevida ou ilicitamente poderão ensejar condutas altamente discriminatórias.

Esta categoria fora, primeiramente, apresentada pelo art. 6º, do Convenção 108/1981 (UNIÃO EUROPEIA, 1981), do Conselho da Europa, que dispõe quanto à proibição do tratamento e utilização dos dados sensíveis.

#### Artigo 6º - Categorias especiais de dados

Os dados de carácter pessoal que revelem a origem racial, as opiniões políticas, as convicções religiosas ou outras, bem como os dados de carácter pessoal relativos à saúde ou à vida sexual, só poderão ser objeto de tratamento automatizado desde que o direito interno preveja garantias adequadas. O mesmo vale para os dados de carácter pessoal relativos a condenações penais.

O art. 8º da Diretiva Europeia 95/46/CE (UNIÃO EUROPEIA, 1995) estabelece algumas hipóteses que possibilitam o tratamento de dados sensíveis, dentre as quais quando houver o consentimento explícito do titular dos dados; quando for necessário para proteger interesses vitais do titular ou de terceiros, caso esteja incapaz de dar o consentimento; entre outros.

Logo, é possível afirmar que nos países europeus, após o surgimento da referida categoria, a legislação protetiva de dados tornou-se consideravelmente severa, pois as exigências para o consentimento do indivíduo que deseja dispor de seus dados pessoais foram ampliadas, bem como foram intensificadas as medidas de segurança para o tratamento dos dados pessoais, mesmo após o consentimento.

Além dos dados sensíveis, que são aqueles mencionados no rol da Diretiva 95/46/CE, bem como na Convenção nº 108 do Conselho da Europa, há também a



expressão “tratamento sensível” para dados que não estão incluídos no rol das retrocitadas normas.

Os dados não sensíveis são aqueles que, presumidamente, não causariam constrangimento ao titular, assim como aqueles que não demonstram perspectivas da vida privada do sujeito mesmo sem o seu consentimento. Percebe-se, portanto, que há duas categorias de dados, com igual proteção, quais sejam: os dados sensíveis e os dados pessoais com tratamento sensível.

Existem dados pessoais que, embora a priori demonstrem certa insignificância, podem, após o tratamento, tornarem-se sensíveis pois são potencialmente discriminatórios. Logo, no contexto de processamento eletrônico de dados, é possível afirmar a inexistência de supostos dados insignificantes, pois, na verdade, todos dados após o tratamento ou utilização são potenciais informações e dados discriminatórios.

### 3.2 TÉCNICAS DE PROCESSAMENTO E TRATAMENTO DE DADOS

As técnicas de *data mining*, *profiling*, *data warehouse* e *scoring* são técnicas que possibilitam a obtenção de informações de determinados sujeitos, que são mais utilizados no âmbito consumerista, pois visam a personalização de produtos e diminuição de publicidade. Tais técnicas podem até acarretar benefícios, porém também trazem grandes riscos à privacidade e à discriminação do consumidor, como será visto mais adiante. No entanto, antes de adentrar nas técnicas de tratamento de dados consumeristas, vale demonstrar o processamento e tratamento de dados supostamente inofensivos, mas essencialmente discriminatórios, tais como: dados médicos, listas de trabalhadores e listas de suspeitos.

Após a informatização dos arquivos médicos, os planos de saúde e a prática de medicina se alteraram abruptamente, pois atualmente é possível a coleta e armazenamento de informações do paciente, até mesmo de seu prontuário ou sequência de genes em bancos de dados eletrônicos. Com isso, é facilmente perceptível a relevância da proteção dos dados médicos, uma vez que a relação médico-paciente deve ser pautada em extrema confiança e confidencialidade.

Ainda que haja grande relevância, os dados sintomatológicos de um paciente, prescritos em um prontuário, por exemplo, em nada se comparam aos seus dados genéticos. Portanto, a circulação e o armazenamento de dados genéticos do sujeito devem

possuir extremo sigilo, pois são informações personalíssimas de alto grau privativo. Trata-se de informações que trazem consigo o histórico familiar, informações étnico-raciais do paciente, bem como dados prováveis de eventuais doenças que carrega consigo. Ora, há informações com maior probabilidade de fazer com que o titular sofra discriminações do que estas?

Além disso, quanto aos planos ou seguros de saúde, é possível concluir a seguinte contradição: caso as referidas instituições alcançassem tais dados, só teriam acesso a estes seguros aqueles que não ofereciam nenhum dispêndio, ou seja, aqueles que de fato não precisam do plano de saúde. Por outro lado, aqueles que possuem dados genéticos pendentes a problemas de saúde, graves ou não, ficariam excluídos das referidas instituições securitárias.

Superado o contexto dos dados médicos, passa-se para os dados trabalhistas. No ambiente de trabalho, principalmente nas grandes empresas, há uma prática costumeira altamente discriminatória que seria a elaboração, por parte dos empregados, de uma “lista negra de empregados”. Os empregados que são inseridos na referida lista são aqueles que acionam a Justiça do Trabalho ou por qualquer outro motivo que a empresa não considera positivo.

Essa lista não traz nada de positivo para os trabalhadores, pois só são utilizados com um único fim: dificultar o acesso ao mercado de trabalho dos sujeitos registrados. O caráter discriminatório do uso de tais dados e informações é cristalino, pois eles objetivam impedir o trabalhador de conseguir um emprego somente pelo fato de este exercer seu direito de ação constitucionalmente protegido. Deste modo, a jurisprudência trabalhista brasileira está tendenciosa ao entendimento de que enseja dano moral a inserção de nome do trabalhador em tais listas. Depreende-se este entendimento do seguinte julgado do Tribunal Superior do Trabalho:

**Ementa:** RECURSO DE REVISTA. DANO MORAL. -LISTAS NEGRAS-. OFENSA AO PRINCÍPIO QUE PROTEGE A DIGNIDADE DA PESSOA HUMANA (ARTIGO 1º, INCISO III, DA CONSTITUIÇÃO FEDERAL). PROVIMENTO. A inclusão dos nomes de Empregados nas chamadas -listas negras-, por si só enseja o pagamento de indenização por dano moral, tendo em vista que a prática constitui ofensa ao princípio constitucional que protege a dignidade da pessoa humana (artigo 1º, inciso III, da Constituição Federal), ainda que não haja comprovação no sentido de ter o Autor sofrido prejuízo concreto, no que se refere à conquista de nova colocação no mercado de trabalho. Recurso conhecido e provido para que sejam restabelecidos os comandos da sentença quanto ao deferimento da indenização por dano moral requerida. (Processo: RR - 325/2004-091-09-00.7 Data de Julgamento:

02/04/2008, Relatora Ministra: Maria de Assis Calsing, 4ª Turma, Data de Publicação: DJ 18/04/2008.)

Por fim, no âmbito penal, há ainda a estruturação de listas de suspeitos, que também pode ser considerada como forma de tratamento sensível de dados pessoais. As referidas listas contêm dados com conteúdo altamente discriminatórios que, uma vez divulgados ou usadas inadequadamente pode lesar toda a personalidade do indivíduo, de seu direito à honra ao seu direito à imagem, até mesmo violar diretamente a sua dignidade. Isto porque, um sujeito que é apenas considerado suspeito, mas que depois inocentado, pode ficar marcado como “criminoso” para o resto de sua vida, e essas características influenciam em sua vida pessoal à laboral.

Neste sentido, Cristiano Pinto (2004, p. 239-240) demonstra um episódio da violação da privacidade nesse cenário investigativo. Nos Estados Unidos, no Atentado de 11 de setembro, os agentes do FBI divulgaram na imprensa a existência de uma lista de suspeitos. Durante este mesmo período, fora divulgada em inúmeras páginas da internet uma lista de nomes de pessoas, que continha nomes de sujeitos que apenas foram procurados para fornecer informações à polícia, ao invés de conter os nomes dos suspeitos do atentado. Essa lista continha dados com tratamento altamente sensível, uma vez que violava a privacidade e dignidade dos sujeitos ali contidos, que nada tinham a ver com o evento terrorista.

Quanto as técnicas de armazenamento e processamento de dados que são mais utilizadas no âmbito consumerista tem-se, como já dito: *data warehouse*, *data mining*, *profiling* e *scoring* (MENDES, 2008).

A *data warehouse* é considerada um depósito de dados, em que há um sistema informatizado que armazena grande quantidade de informações. Esse banco de dados tem como objetivo a elaboração de relatórios, bem como o exame de volumes extensos de dados. Esta técnica é encarada como uma base de dados integrados que são orientados pelo sujeito e que possui dimensão não volátil – a orientação pelo sujeito significa que essa base de dados é voltada ao indivíduo, e não para informações operacionais de empresas; considera-se não volátil, pois os dados ali armazenados não são passíveis de alteração, nem cancelamento.

Essa técnica tem como função a tomada de uma decisão estratégica por parte da empresa sobre seus consumidores, pois os dados sobre esses sujeitos são catalogados

conforme a sua relevância, armazenando de acordo com critérios específicos para uma utilização futura pela empresa. A *data warehouse* deve ser subsidiada juntamente com outras técnicas, como a *data mining* e a *profiling*.

A *data mining*, também denominada de mineração de dados, é utilizado para os dados de difícil compreensão que, através de seu devido processamento, são transformados em informações úteis para a empresa. O retrocitado tratamento é realizado através de combinação de dados e estatísticas, ou seja, a empresa combina e une dados que inicialmente são primitivos acerca daquela pessoa, formando novas informações valiosas.

A mineração de dados tem como objetivo a criação de padrões de classificação de pessoas, ordenando e transformando um banco de dados por meio de uma extração de inteligência. Com isso, é possível afirmar a existência de um risco discriminatório dessa técnica, visto que a segmentação e classificação de pessoas, pode gerar uma análise rotulada de sujeitos, discriminando-os. Embora a conclusão lógica seja a de que a técnica, per si, leva a discriminação das pessoas, na verdade, é o seu modo de utilização e as decisões tomadas conforme as informações extraídas por tal banco dados que podem ser consideradas discriminatórias.

A técnica denominada *profiling* é uma verdadeira construção de perfil do sujeito, ou seja, um registro completo sobre a personalidade e imagem do indivíduo. Logo, a *profiling* é a reunião de dados sobre a mesma pessoa, objetivando construir uma imagem detalhada sobre ela para que assim seja criado um padrão de comportamento, hábitos e preferências consumerista, ou seja, torna a pessoa completamente previsível.

Laura Mendes (2008, p. 105-106) sobre o tema apresenta relevante informação, trazendo, inclusive, o entendimento do autor Matthias Schwenke, de sua obra *Individualisierung und Datenschutz*:

Os riscos da técnica de construção de perfis não residem na sua grande capacidade de junção de dados; na realidade, a ameaça consiste exatamente na sua enorme capacidade de combinar diversos dados de forma inteligente, formando novos elementos informativos. Nesse sentido, é o entendimento de Matthias Schwenke, que afirma como a construção de perfis pode ser ameaçadora à personalidade e integridade do cidadão-consumidor: “A criação de perfis dos consumidores é problemática em diversos aspectos: perfis apresentam riscos à esfera privada e íntima, uma vez que possibilitam a manipulação relativa à sua vontade, bem como ensejam o mau uso dos dados no perfil. Problemático é também que o perfil seja criado sem o conhecimento e o consentimento do consumidor, sem que sejam asseguradas adequada proteção do sujeito submetido a essa técnica”.

Por fim, a técnica *scoring* é considerada um verdadeiro sistema de avaliação do consumidor, que conta como objetivo reconhecer os consumidores das empresas que possuem maior valor, no sentido de encaminhá-los informativos de promoções de seu interesses e contratos de fidelização. Por óbvio, a conclusão é a de que para se chegar em uma lista de “melhores consumidores”, tem-se que separá-los dos “piores consumidores”, os quais não recebem ofertas tão vantajosas, não recebem planos de fidelização, entre outras estratégias da empresa.

No Brasil, essas listas de “piores consumidores” são elaboradas principalmente pelo SERASA e o Experian Brazil. A má utilização de tais sistemas pode causar altos danos aos sujeitos, quanto aos seus direitos da personalidade. Isto porque o cadastro de “maus pagadores” no Brasil inviabiliza o sujeito de conseguir ofertas satisfatórias, bem como a compra de créditos ou financiamentos. Desta forma, deve ser assegurado ao titular dos dados um mínimo de controle e participação nas decisões que são tomadas a seu respeito com fundamentos nos dados que estão contidos nestas listas, pois, como já demonstrado, esses dados afetam significativamente oportunidades que eventualmente lhe seriam concedidas.

Catarina Sarmento e Castro (2005, p. 252) fazendo uma alusão à Diretiva 95/46/CE, afirma:

A previsão do art. 13º, no. 1, da Lei de Proteção de Dados, que segue de perto a redação da Diretiva 95/46/CE, teve como um dos seus objetivos a proibição do *credit scoring* que consiste na ‘atribuição ou denegação automática de crédito pessoal, consoante a pessoa que solicita esse crédito responde ou não a certas características pessoais ou profissionais, previamente definidas no programa de computador.(...) Esse art. 13º, no. 1, da Lei de Proteção de Dados não impede, de modo absoluto, a utilização de operações de triagem e seleção realizadas a partir de um tratamento automatizado de dados pessoais. Admite-se que os dados armazenados de forma automatizada possam ser utilizados para ajudar uma tomada de decisão, v.g. fornecendo mais informação, ou seguindo a atuação apropriada, mas os computadores e os dados que armazenam não devem ser utilizados como único meio para encontrar a solução.

Do que é explicitado pela retrocitada autora, infere-se que os dados incluídos em *scoring* poderão ser utilizados apenas para auxiliar uma tomada de decisão, desde que bem fundamentada, ou seja, a decisão referendada somente com a afirmação de tais dados não deve ser considerada válida.

Em razão de todas as tecnologias e técnicas de processamento de dados, percebe-se que esse novo contexto virtual potencializa as violações e ameaças a privacidade e a intimidade dos sujeitos. Tais violações podem ocorrer pela simples divulgação do nome,

imagem ou dados não sensíveis sem o devido consentimento do titular, bem como a sua inserção em cadastros, disponibilizados abertamente ou não para a sociedade.

A problemática brasileira se instala na perspectiva de que a legislação nacional não está se adaptando a essa nova realidade de forma satisfatória. Isto porque, a velocidade que essas técnicas e tecnologias são criadas e colocadas no meio social não é proporcional ao trabalho legislativo brasileiro. Logo, será demonstrado a seguir, de forma comparativa, que o ordenamento nacional não está adequado de forma a garantir eficazmente a proteção de dados pessoais.

Portanto, é possível afirmar que essa nova dinâmica e fluidez do contexto social atual reflete diretamente na privacidade e intimidade dos sujeitos, fazendo que com sejam necessárias formas de tutelas distintas das que são oferecidas atualmente. Deste modo, faz-se necessária compreender os meios regulatórios já estabelecidos em países estrangeiros, compreendendo a forma de tutela da privacidade e da intimidade perante os dados pessoais.

## **4 MEIOS DE TUTELA E DE PROTEÇÃO INTERNACIONAIS DOS DADOS PESSOAIS**

Como já demonstrado em todos os capítulos anteriores, os dados e as informações têm conquistado espaços cada vez mais relevantes em nossa sociedade, fazendo com que, conseqüentemente, o direito à privacidade e a proteção destes dados ocupem posição de destaque no ordenamento jurídico.

Com isso, sendo delimitada a constituição do direito à privacidade como um direito fundamental perante o Direito Civil-Constitucional, bem como depois de traçados os principais instrumentos e formas de processamentos utilizados pela tecnologia da informação, neste momento serão demonstrados os modelos de proteção dos dados pessoais como forma de garantir o retrocitado direito fundamental.

O modelo regulatório da União Europeia é o mais influente na conjuntura internacional a respeito do tema da privacidade sobre os dados pessoais. No entanto, boa parte dos modelos regulatórios atuais possui viés garantista e protetivo dos usuários, esquecendo de regular as empresas de forma que estas cumpram suas obrigações, para que assim a sociedade passe a considerar a privacidade com um direito, de fato, fundamental.

Será, inicialmente, demonstrada a conjuntura internacional dos modelos regulatórios para a proteção dos dados pessoais, demonstrando as estratégias regulatórias que são utilizadas por alguns países. Em seguida, no capítulo seguinte, serão traçadas algumas perspectivas para a construção de um marco regulatório de dados pessoais com fulcro na privacidade no ordenamento brasileiro.

### **4.1 A CONFLUÊNCIA INTERNACIONAL NA POLÍTICA DE PROTEÇÃO DE DADOS**

Os debates sobre a proteção de dados pessoais se iniciaram em meados da década de 60 e 70, no momento em que alguns governos, como os Estados Unidos e alguns Estados-Membros da União Europeia, tentaram instituir um único banco de dados da nação, visando centralizar tantos outros bancos de dados. No entanto, a população europeia e norte-americana não estava de acordo com essa política governamental, o que motivou as mais diversas reações populares – inclusive, essa reação popular ensejou a

primeira geração de normas protecionistas referentes a dados pessoais, conforme será explicitado mais adiante.

Neste diapasão, é possível citar o caso do *National Data Center*, de 1965, que foi um projeto do Poder Público norte-americano, que tentou instituir um órgão que centralizasse todos os dados da população. Este órgão seria o único banco de dados do país, o que, conseqüentemente, desobrigava os demais órgãos governamentais que focassem seus investimentos em tecnologias de armazenamento.

O *National Data Center* também possibilitaria a realização de estatísticas veloz e precisamente, de modo que as correções ou rastreio de dados dos cidadãos seriam mais fáceis. Além do mais, tais dados reunidos seriam utilizados com uma eficiência fenomenal para as mais diversas atividades públicas, seja para tomada de decisões ou planejamentos de políticas públicas.

O projeto de criação do referido órgão foi evoluindo de tal maneira, que o governo chegou à conclusão de que este centro deveria reunir todos os dados dos americanos, seja em relação ao nascimento, registro escolar, benefício previdenciário, impostos, registros criminais, serviço militar, entre outros. A partir de então, a população passou a discordar veemente de tal conduta do Poder Público, no qual culminou em debates no Congresso Americano sobre pontos positivos e negativos do órgão.

Com isso, chegou-se à conclusão de que o *National Data Center*, ao centralizar os dados, ocasionaria fortes lesões aos direitos fundamentais, pois conferiria um poder imensurável à Administração Pública norte-americana, ao torná-la detentora de todas as informações da vida de cada cidadão, lesionando a sua política liberal, que é tão tradicional. Portanto, esse projeto do governo norte-americano nunca chegou a se concretizar devido às pressões sociais realizadas, bem como a verificação de forte lesão ao direito fundamental à privacidade.

Além deste exemplo norte-americano, vale ressaltar um caso similar que ocorreu na França, em 1970, ao instituir o denominado projeto SAFARI (*Système Automatisé pour lês Fichiers Administratifs et lê Répertoire de Individus*). Esse sistema trataria cada cidadão francês por um número, reunindo-os todos em um único órgão dentro do Instituto Nacional de Estatística francês.



Entretanto, assim como os norte-americanos, os franceses pressionaram o seu governo, sob alegação de que esse sistema lesionaria abruptamente seu direito à privacidade e, com isso, o projeto também não foi concretizado. Inclusive, após esse debate popular, em 1978, o Poder Legislativo francês foi na via contrária ao SAFARI, ao aprovar uma lei de proteção de dados pessoais, a Lei nº 78-77 (FRANÇA, 1978) que dispõe sobre informações, ficheiros e liberdades.

Mendes (2008, p.30-31) sobre a criação pelo Poder Público de bancos de dados centralizados informa:

Esses projetos para a construção de grandes bancos de dados nacionais não lograram êxito, não apenas em razão da sua rejeição pelos cidadãos, mas principalmente, porque a tecnologia desenvolveu-se por outro caminho. Ao invés da criação de um único banco de dados, foram desenvolvidas técnicas para permitir o processamento de dados de forma descentralizada, como os “minicomputers”, o que transformou completamente o debate sobre a proteção de dados pessoais. Juntamente com os planos de construir bancos de dados centralizados, os governos também buscaram desenvolver números de identificação pessoal para cada cidadão, o que também foi motivo de forte reação dos cidadãos americanos e dos países europeus. Esses números universais serviriam para ampliar a eficiência da Administração Pública, facilitar a comunicação, ampliar a conectividade com outros bancos de dados e aumentar a acuidade das informações dos cidadãos armazenadas pelo Estado.

Portanto, diante das inúmeras explosões legislativas na tentativa de centralizar dados pessoais, colocando todos à disposição do governo e após a pressão popular contra os referidos projetos, fez com que surgisse o debate quanto à necessidade de uma regulamentação legislativa na contramão, ou seja, sobre a proteção de dados pessoais.

Quanto às legislações protecionistas de informações pessoais dos mais diversos países, é possível perceber uma convergência nos meios de tutela mais do que divergências entre eles. Na verdade, essa convergência ultrapassa o conceito de semelhança legislativa, sendo verificado um padrão vanguardista das referidas normas, pois todas elas contam com institutos e instrumentos semelhantes, ainda que com as particularidades de cada ordenamento.

É um tanto complexo restringir a proteção de dados pessoais a um conceito único, pois esse assunto é uma construção histórica, no qual se altera conforme as transformações tecnológicas que são colocadas em sociedade, fazendo com que a legislação esteja sempre se adaptando ao tema. Os países europeus e a União Europeia, a partir da década 70, tiveram maior influência para criar as regulamentações no que concerne a proteção de dados.

Viktor Mayer-Schönberger, em sua obra *Generational Development of Data Protection in Europe* (2001), realizou uma divisão das legislações europeias de proteção de dados pessoais em gerações, as quais serão delineadas a seguir. Em meados de 1970, surgiu a primeira geração das retrocitadas normas protecionistas, sendo o reflexo dos processamentos eletrônicos de dados por parte do Poder Público e empresas privadas, bem como a reação das tentativas de centralização de bancos de dados nacionais, como já explicado.

Deste modo, os Governos europeus passaram a fazer uso de uma tecnologia de armazenamento, coleta e processamento de dados, fazendo com que surgisse uma reação popular contrária a essa política, pois era temido que surgisse um controle absoluto sobre os cidadãos através de uma burocracia altamente informatizada. Por isso, conforme Mayer-Schönberger, a primeira geração de normas de proteção de dados tem um viés funcional, no qual busca controlar os bancos de dados, de modo que seu funcionamento dependa de uma licença prévia dos titulares ou registro nos órgãos públicos competentes. São exemplos de normas de proteção de bancos de dados de primeira geração: Lei Federal de Proteção de Dados da Alemanha (1977); Estatuto de Proteção de Dados do Estado Alemão (1974); Lei de Dados da Suécia (1973).

Ainda que os projetos que instituíam os bancos de dados centralizados e públicos não tenham se concretizado, em razão das normas de primeira geração, a transformação e desenvolvimento da tecnologia possibilitou o surgimento de bancos de dados descentralizados, que seriam utilizados por unidades organizacionais de governo separadamente, bem como pela iniciativa privada. Logo, houve um grande crescimento de pequenos bancos de dados, que tornou a legislação vigente frágil, surgindo, portanto, a necessidade de sua alteração.

A segunda geração de normas de proteção de dados pessoais surgiu nesse cenário de proliferação de pequenos bancos de dados, visando a proteção do direito à privacidade de forma prioritária, ao invés de regulamentar tão somente os procedimentos que eram operacionalizados. Então, neste momento histórico, a proteção de dados pessoais se vinculou diretamente ao direito à privacidade, isto é, a privacidade informacional – já estudada anteriormente – passou a ser inserida em alguns textos Constitucionais, tais como a Constituição Austríaca, Constituição Espanhola e Constituição Portuguesa.

Perceba-se que o enfoque da legislação era a de permitir que o titular participasse da coleta e processamento de seus dados, através do consentimento, ou seja, as normas de segunda geração conferem ao cidadão o poder de interferência no que concerne à privacidade informacional de sua titularidade. Isto ocorreu porque a preocupação da população não era mais a instituição de um único banco de dados do Poder Público, mas a existência de milhares de bancos de dados disseminados em todo o mundo e, todos eles, conectados através de uma rede.

Quanto as características das normas de segunda geração, Mayer-Schönberger (2001) aduz da seguinte maneira:

Primeiramente, algumas das instituições de segunda geração não apenas investigavam as ofensas à proteção de dados pessoais, mas também se tornaram uma espécie de ombudsman<sup>3</sup> da proteção de dados pessoais para os cidadãos. Quando os direitos individuais eram violados, os cidadãos deveriam poder se reportar a alguma instituição – uma instituição que de algum modo poderia ajudá-los a reforçar o direito individual à proteção de dados pessoais. Segundo, algumas das instituições de segunda geração transformaram-se em órgãos adjudicatórios que concediam opiniões de como a burocracia poderia ou não interpretar as normas de proteção de dados pessoais.

A terceira geração de normas de proteção de normas pessoais surgiu com a decisão da Corte Alemã acerca da Lei do Censo em 1983. O Tribunal Constitucional Alemão trouxe para o seu ordenamento jurídico o direito à autodeterminação informativa, alterando drasticamente a forma de consentimento dado pelo titular quando seus dados fossem objeto de processamento ou armazenamento. Na verdade, a terceira geração é marcada por uma nova interpretação dada as legislações já existentes, pois torna possível a participação integral do titular no processamento de seus dados, ou seja, o cidadão está envolvido na coleta, armazenamento, transmissão, entre outras formas de processamento.

Já a quarta e última geração de normas de proteção aos dados pessoais conta como principal finalidade tornar a participação do sujeito ainda mais forte sobre seus dados. Além disso, passaram a existir alguns dados que deveriam escapar do controle do particular, isto porque, por serem tão sigilosos e dizerem respeito a direitos fundamentais, não podiam estar inseridos na esfera de disposição individual. Percebe-se que esta geração de normas está presente nos dados pessoais sensíveis, já estudados no capítulo anterior.

---

<sup>3</sup> O termo “ombudsman”, de origem nórdica, se refere a uma função encarregada de defender os direitos da população e dos cidadãos, em si, através de investigação após o recebimento de queixas e denúncias de abuso de poder ou má prestação de serviço por parte de servidores ou instituições públicas. No Brasil, pode-se afirmar que este seria o cargo de Ouvidor das instituições públicas e privadas.

Os dados sensíveis, que possuem alto conteúdo discriminatório, fizeram com que alguns países proibissem totalmente o uso e a disposição de tais informações como as legislações da Noruega, França e Grã-Bretanha. Entretanto, as legislações alemã e Diretiva Europeia de 95/46/CE (UNIÃO EUROPEIA, 1995) não proíbem de forma absoluta o processamento de dados sensíveis, mas o restringe tão somente. Mendes (2008), ao tratar do tema, chega à seguinte conclusão:

É bastante provável que as normas de proteção de dados pessoais continuem a se transformar e a se adaptar às novas realidades sociais. Assim, é possível se fazer algumas previsões. Cada vez mais é provável que todas as legislações na Europa se tornem mais homogêneas, sempre com um alto nível de proteção individual, principalmente em razão do intenso fluxo transfronteiriço de informações e das exigências econômicas globais. Ademais, os direitos de participação tendem a ser ampliados, na medida em que novas tecnologias de comunicação permitem cada vez mais a participação do indivíduo no momento do processamento de seus dados pessoais. Por fim, é provável que diante do fluxo de informações pessoais entre países, as normas nacionais de proteção de dados pessoais sejam enfraquecidas, ampliando a força de regulamentações regionais.

Tem-se que as modificações legislativas ocorreram principalmente entre 1970 e 1990, décadas nas quais o desenvolvimento tecnológico cresceu de forma exponencial. Com isso, é possível concluir que o sistema de proteção de dados pessoais em tais países viabilizou a proteção a liberdade e igualdade, com enfoque na autodeterminação informativa, principalmente no que concerne a proibição ou restrição no processamento de dados sensíveis.

Discorrido sobre toda a legislação internacional de forma cronológica, bem como o seu entendimento doutrinário através da divisão em gerações legislativas, passa-se, a seguir, para o estudo dos modelos internacionais *in loco* das normas de proteção de dados pessoais.

#### 4.2 MODELOS REFERÊNCIAS DE REGULAÇÃO E PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO INTERNACIONAL

A presente seção visa demonstrar as estratégias regulatórias que estão postas de fato nos ordenamentos jurídicos estrangeiros, partindo da premissa de que é necessária a tutela dos dados pessoais e do direito à privacidade. A seguir serão analisados, brevemente, os modelos europeu, norte-americano e uruguaio, os quais guardam distinções entre si relevantes para o estudo dos dados pessoais.

O modelo europeu, em si, é o modelo mais tradicional dentre os demais, no qual foi usado como grande influenciador dos demais ordenamentos por ser fundamentado em

uma abordagem personalista dos direitos fundamentais. Já o modelo norte-americano encontra-se na contramão do retrocitado, pois está sustentado nos princípios da liberdade contratual e propriedade privada. Por fim, o modelo uruguaio foi influenciado pelo modelo tradicional europeu, porém com algumas adaptações relevantes para a realidade da América Latina.

#### **4.2.1 Sistema Regulatório Europeu**

Diante de tudo que foi estudado no presente trabalho, observa-se que o modelo europeu sempre esteve à frente dos demais no que diz respeito à proteção de dados pessoais. Por exemplo, a Convenção nº 108 (UNIÃO EUROPEIA, 1981) do Conselho Europeu fundou um autêntico sistema de tutela que serve como referência para toda a comunidade internacional.

O Sistema jurídico atual da União Europeia conta com institutos como: diretivas; regulamentos; orientações; e decisões vinculantes<sup>4</sup>, dos mais diversos níveis hierárquicos, nos quais estabelecem normas específicas sobre direitos e obrigações a respeito dos dados pessoais, desde que embasadas em orientações gerais europeias.

A tão mencionada Diretiva 95/46/CE (UNIÃO EUROPEIA, 1995) é considerada como norma central e básica de todo sistema europeu de proteção de dados pessoais. Isto porque, na referida norma estão contidos os principais conceitos deste tema; traz consigo princípios norteadores para tutela dos dados pessoais, seja para coleta, manipulação, armazenamento, entre outros, ou seja, princípios para todo o tratamento de dados pessoais; ainda, arrola os direitos básicos dos titulares de dados pessoais, tratados ou não.

A Diretiva 2002/58/CE (UNIÃO EUROPEIA, 2002) do Parlamento e Conselho Europeu, regulamenta o setor de comunicações, quando este realizar tratamentos de dados pessoais, e rege a proteção da privacidade neste mesmo setor. Esta norma envolve em seu conteúdo questões acerca da conservação dos dados de conexão no que concerne ao faturamento de serviços de internet prestados; a utilização de lista públicas, como as listas

---

<sup>4</sup> Vale ressaltar quanto a natureza jurídica das normas da União Europeia. As Diretivas são normas instituídas pela Comissão Europeia ou Parlamento Europeu, em que é determinado uma meta a ser alcançada pelos Estados-membros, cabendo a cada um deles instituir a forma como essa meta será atingida, desde que respeitados os princípios norteadores da norma supranacional. Já os Regulamentos são legislações aplicáveis de forma direta a todos os países membros, seja pessoa física ou jurídica, se valendo do direito como se este fosse nacional. As orientações são atos que não possuem força vinculante, mas com conteúdo recomendável a se aplicar ou evitar. Por fim, as Decisões são atos com força vinculante, contudo esta força é aplicável apenas para partes envolvidas na relação jurídica, seja Estado-membro ou empresa privada.

telefônicas, por exemplo; o envio de mensagens não solicitadas, denominadas como spam.

Além das diretivas, sabe-se que as decisões do Parlamento e do Conselho também são consideradas propostas normativas com força vinculante, que, inclusive, por terem a possibilidade de revisão e atualização, são mais facilmente detalhadas sobre o tema de dados pessoais, que possui forte fluidez.

A Decisão da Comissão 2001/497/CE (UNIÃO EUROPEIA, 2001) tem em seu teor a existência de cláusulas protecionistas para os interessados em transferir seus dados para países estrangeiros à União Europeia. Tais cláusulas visavam algumas garantias suficientes para que fosse respeitada a Diretiva 95/46/CE (UNIÃO EUROPEIA, 1995), preservando os dados a transferidos aos estrangeiros. Inclusive, em 2004, essa decisão foi alterada, pois foram introduzidas novas espécies de cláusulas protecionistas, ou seja, foi ampliado o rol de garantias dos dados pessoais – isso demonstra o caráter fluído dessas decisões, que são capazes de se amoldar as alterações sociais.

Um grande avanço na legislação europeia, surgiu com o Regulamento nº 679 de 2016 (UNIÃO EUROPEIA, 2016), do Parlamento e do Conselho Europeu, conhecido como Regulamento Geral de Proteção de Dados – *General Data Protection Regulation* ou GDPR. Este regulamento surgiu como forma de substituir a Diretiva 95/46/CE, pois em seu texto há a união de todas as normas de proteção de dados pessoais. O avanço de tal norma se encontra na possibilidade de aplicação direta como se fosse uma norma interna do país, reduzindo, portanto, a fragmentação do sistema de proteção de dados pessoais – isto porque, antes era necessária a incorporação do texto supranacional no ordenamento interno.

Guilherme Guidi (2017, p. 9-10), sobre a organização das normas de proteção de dados, leciona:

Estruturadas como se encontram, as normas comunitárias básicas sobre a proteção de dados fornecem uma estrutura onde (i) os valores fundantes - cuja atualização não precisa seguir o ritmo da tecnologia - estão bem fixados em normas gerais, que costumam apresentar também maiores dificuldades para sua alteração; (ii) os princípios e subprincípios em que se traduzem tais valores são bem desenhados e fixados em normas ainda de caráter geral, mas tecnologicamente neutras - o que garante que possam ser aplicadas ainda que com mudanças razoáveis no campo tecnológico; e (iii) regras específicas criadas pelo sopesamento e fixação legal desses princípios, são erigidas em normas de caráter específico e sujeitas a um procedimento simplificado de produção e atualização - permitindo que, ainda que não absolutamente

tecnologicamente neutras, sigam a curta distância o desenvolvimento tecnológico.

Essa estrutura normativa hierarquizada tem como ponto fulminante de suas regras, valores e princípios a sincronia entre a lei e a realidade. Isto porque, em um contexto de rápida alteração e evolução, que é o caso dos dados pessoais e seu desenvolvimento tecnológico, é fundamental que a legislação foque seus esforços para um patamar de aplicabilidade com atualização constante das normas, de forma que acompanhem as alterações das tecnologias.

#### **4.2.2 Sistema Regulatório Norte-americano**

Diferentemente do ordenamento europeu, os norte-americanos não possuem uma lei federal geral para proteção dos dados pessoais, que defina os princípios e regras comuns, unificando os direitos relativos aos dados pessoais dos cidadãos estadunidenses.

Na verdade, os Estados Unidos optaram por dar um tratamento específico e setorial à esta matéria, pois, na verdade, possui leis de âmbito nacional que disciplinam o uso de dados pessoais de crianças e adolescentes; a proteção de alguns dados sensíveis, dentre eles os dados médicos, de saúde, financeiros; entre outras. Além disso, diante da forma de federação norte-americana, alguns estados também possuem legislação específica que versa sobre o direito à privacidade e a proteção de dados pessoais.

Algumas leis do Poder Legislativo dos Estados Unidos devem ser destacadas, dentre elas: O *Privacy Act* (ESTADOS UNIDOS, 1974) versa sobre alguns regramentos e princípios para o armazenamento, coleta, uso e tratamento de dados pessoais no campo das atividades do setor público federal. A referida legislação dispõe sobre as hipóteses em que há a publicação de dados pessoais para outras agências públicas ou terceiros, devendo, nestes casos, o titular consentir ou, ao menos, haver interesse público para tal conduta.

O *Wiretap Act* (ESTADOS UNIDOS, 1986) versa sobre a proibição de interceptação, uso ou revelação de quaisquer espécies de comunicação, seja telefônica ou eletrônica. Esta lei se refere aos dados que estão fluídos, ou seja, uma comunicação em fluxo. Já a *Stored Communications Act* (ESTADOS UNIDOS, 1986) protege os dados que não estão mais em fluxo, ou seja, as comunicações armazenadas, que já foram recebidas ou enviadas. Refere-se a dados de cadastro, por exemplo, que são armazenadas

por prestadores de serviços, como as informações acerca do nome, endereço, documentos, entre outros.

Há o *Pen Register Act* (ESTADOS UNIDOS, 1986) que regula especificamente atos do Poder Público, relativo às condutas que se utilizam de dispositivos de rastreamento de chamadas. Esses dispositivos são denominados de *pen registres*, e têm a capacidade de identificar tão somente os terminais de chamadas telefônicas, pois não viabiliza o conteúdo da comunicação. Vale o adendo de que essas três leis supracitadas foram reunidas pela lei federal denominada de *Electronic Communications Privacy Act* (ESTADOS UNIDOS, 1986).

No campo da saúde, há o *Health Insurance Portability and Accountability Act* (ESTADOS UNIDOS, 1996) que estabelece regramentos relativos à proteção de dados médicos garantindo a privacidade em âmbito federal. A referida legislação dispõe sobre padrões de segurança de dados relacionados à saúde que estão estabelecidos em dispositivos eletrônicos; sobre a obrigação, nos casos de exposição ou lesão a dados pessoais, de notificar os seus titulares; sobre as hipóteses em que são necessárias ou não o consentimento do titular dos dados pessoais para a sua utilização ou tratamento; entre outras disposições.

O ordenamento norte-americano não possui uma única autoridade com função e dedicação exclusiva de proteger os dados pessoais e a privacidade dos titulares. Na verdade, existem órgãos esparsos que são responsáveis pela aplicação das leis vigentes, bem como de fiscalização e sanção – seriam como as agências reguladoras, se comparadas com o ordenamento brasileiro. A atuação de tais órgãos de proteção é separada e complementemente independente, de maneira que não serão necessariamente homogêneos em suas condutas, bem como seus posicionamentos nem sempre convergirão sobre algum instituto ou conceito.

Importante ressaltar que a atuação dos retrocitados órgãos deve caminhar junto ao Poder Judiciário, pois, para que suas decisões sejam cumpridas, é necessário recorrer a um processo judicial. Portanto, percebe-se que, além da ausência de leis gerais de proteção de dados, as poucas existentes não conseguem ter eficácia imediata, tendo em vista a necessidades de precedentes judiciais.

Logo, resta cristalino que o sistema regulatório norte-americano de proteção de dados em nada se parece com o modelo tradicional europeu. Isto porque, ainda que seja



reconhecido pelo ordenamento que exista uma garantia de proteção aos dados pessoais devido à proximidade que estes estão em lesionar a privacidade, a tutela destes direitos não é autoaplicável ou facilmente demandada contra aqueles que efetuam o tratamento de dados pessoais.

Devido ao alto valor da liberdade, quase que absoluta, no sistema estadunidense, o que rege a coleta e a utilização de dados pessoais, geralmente, é o contrato celebrado entre o titular e a empresa, por exemplo. Logo, o instituto jurídico mais relevante para os norte-americanos é o consentimento do titular, que mais se aproxima de uma forma de venda de informações do que, de fato, uma maneira de resultado que o titular pretende que seja feito com seus dados.

Em outras palavras, no modelo regulatório tradicional o consentimento deve ser informado e expresso, devendo o titular ao consentir tomar conhecimento dos benefícios e malefícios que o tratamento dos seus dados pode fazer, enquanto que o consentimento norte-americano é mera transação de informação que é efetuada entre uma relação de comércio entre o usuário dos dados e o responsável pelo tratamento destes.

Deste modo, percebe-se que, havendo uma transação de dados pessoais, entre um indivíduo comum e uma grande empresa, existirá claramente uma relação de disparidade, um desequilíbrio contratual, que pode levar a circunstâncias abusivas sem a devida proteção legal. Com isso, na ausência de legislações autoaplicáveis, bem como não havendo uma norma geral, a consequência é única: judicialização de tais problemáticas.

Em uma breve análise sobre este sistema regulatório, tem-se uma forte garantia da livre iniciativa e princípio da liberdade, bem como garante-se a inovação tecnológica, pois é possível a utilização de formas inovadoras, ainda que não reguladas, em respeito aos retrocitados princípios. Entretanto, quanto à proteção dos dados pessoais e privacidade do titular, é possível afirmar que é um sistema não tão eficaz, uma vez que a regulação dependerá, ao final, do Judiciário, que deverá realizar uma ponderação entre dois princípios americanos aparentemente contraditórios: o direito à privacidade e o direito à livre iniciativa.

#### **4.2.3 Sistema Regulatório Uruguaio**

O último modelo referência estrangeiro é o sistema regulatório uruguaio, que demonstra relevância para o presente trabalho, por ser um país de história semelhante à

brasileira. Isto porque, o seu ordenamento jurídico é resultado de uma reafirmação e ampliação dos direitos fundamentais, após um regime ditatorial – durante uma ditadura é comum que haja a reunião de dados sobre cidadãos, principalmente sobre aqueles que são contrários ao regime. Logo, a reafirmação da democracia e dos direitos fundamentais é tradição no sistema uruguaio e, por isso, demonstra-se relevante analisar alguns traços da proteção dos dados pessoais e da privacidade neste ordenamento jurídico.

Doneda (2006, p. 327-328) leciona sobre o tema:

Sinteticamente, apontamos o fato de que um instituto do gênero tenha uma especial razão de ser em sociedades recém-saídas de regimes ditatoriais, como era o panorama em muitos países latino-americanos na década de 1980 em diante, em cuja sociedade civil persistia o trauma pelo uso autoritário da informação. Em um momento posterior ao fim destes regimes, um instrumento para a requisição das informações pessoais em mãos do poder público, em particular pelos órgãos diretamente encarregados pela repressão à atividades insurrecionais, era tanto desejado quanto necessário, seja para a tutela dos direitos fundamentais envolvidos como também pelo seu importante papel na formação de uma cultura democrática. Com tal escopo foi concebido o *habeas data* - para proporcionar, portanto, ao cidadão um instrumento para conhecer diretamente e, se necessário, retificar as informações sobre sua própria pessoa armazenadas em bancos de dados [de caráter público].

A principal fonte normativa sobre o sistema de tutela é a Lei nº 18.331 de 2008 (URUGUAI, 2008) que dispõe sobre a proteção de dados pessoais dos cidadãos uruguaios e sobre uma ação denominada *Habeas Data*. Trata-se de uma lei geral, com princípios e regramentos, sobre a proteção de dados pessoais no contexto de coleta, tratamento e utilização destes. Inclusive, esta lei institui um órgão de controle de dados pessoais denominado de *Unidad Reguladora y de Control de Datos Personales*, que consiste numa verdadeira autoridade específica com função de proteger os dados pessoais dos uruguaios. A atuação deste órgão está pautada na emissão de normativas como forma de interpretar e integrar os regramentos contidos na legislação uruguaia.

Com isso, a mesma lei traz consigo a garantia do direito à informação, bem como o acesso, supressão e retificação de dados; tutela específica para a categoria de dados sensíveis; dispõe especificamente sobre a utilização de dados para fins publicitários, bancos de dados consumeristas; entre outras disposições. Além disso, traz regramentos processuais sobre a ação *Habeas Data*.

O Decreto nº 414/2009 (URUGUAI, 2009) regulamentou a Lei nº 18.331/2008, pois dispõe minuciosamente sobre os dados pessoais e a sua proteção. Este decreto dispõe sobre especificações quanto ao exercício dos direitos de acesso, retificação, eliminação ou supressão de dados pessoais; detalha a forma de comunicação do consentimento do

titular para o tratamento de seus dados; entre outros. Além disso, o ordenamento uruguaio conta com alguns decretos específicos que versam sobre os dados pessoais referentes a saúde e dados pessoais que estão expostos em meios informáticos, que são, respectivamente, o Decreto nº 396 de 2003 (URUGUAI, 2003) e Decreto nº 249 de 2007 (URUGUAI, 2007).

A Lei nº 18.331 (URUGUAI, 2008) teve como inspiração a norma geral de regulação dos dados pessoais europeu, a Diretiva 95/46/CE. É possível afirmar que o modelo uruguaio guarda similaridade com o modelo tradicional europeu, principalmente no que concerne a existência de uma lei geral que verse sobre os principais regramentos e princípios da proteção de dados pessoais, ainda que estes sejam desenvolvidos e minuciados através de decretos regulamentadores.

A existência do órgão regulador para proteção de dados pessoais mostra, claramente, a disparidade do modelo uruguaio com o modelo norte-americano, pois o primeiro conta com a centralização de competências, enquanto que o segundo não protege os dados pessoais desta forma. O órgão de autoridade de proteção de dados uruguaio faz com que haja um controle anterior ao tratamento de dados pessoais, realizando através de medidas de segurança nas bases de dados e no destino dos dados nas hipóteses de comunicação.

A autoridade de proteção de dados tem a competência de fiscalizar o cumprimento da lei geral, através de denúncias, inspeções ou solicitações de dados, podendo, inclusive, havendo violação, aplicar sanções administrativas – advertências, multas, suspensão do banco de dados. Ainda, vale ressaltar que o referido órgão uruguaio não tem poder decisório jurisdicional e, verificando um conflito entre um órgão (público ou privado) e um cidadão, deverá indica-lo quais os meios que estão a sua disposição para tutelar seu direito. Sobre este ponto, Guidi (2017, p.18) esclarece:

Não há, pois, uma instância administrativa dedicada a questões relacionadas a proteção de dados, sendo tais casos direcionados ao Poder Judiciário em geral, que pode ser acionado exclusivamente pelo titular dos dados. [...] É verdade que a Unidad Reguladora y de Control de Datos Personales pode, com base em uma denúncia de violação de um direito garantido em lei, realizar uma inspeção e sancionar a empresa em falta. No entanto, seu provimento será sempre limitado à aplicação de uma das três sanções descritas na lei, não podendo a Autoridade determinar, por exemplo, que a empresa adote determinado comportamento ou tome as providências para garantir determinado direito. A Autoridade de Proteção pode simplesmente autuar as violações da lei, cabendo ao Poder Judiciário qualquer provimento positivo para obrigar a empresa violadora a garantir certo direito.

Diante desta realidade de judicialização nas hipóteses em que há lide que verse sobre dados pessoais, o Uruguai criou uma ação específica para tutelar, o Habeas Data. Este remédio processual proporciona a possibilidade de o titular tenha conhecimento sobre os dados relativos a si, bem como o uso e a finalidade destes, desde que estejam em bancos de dados públicos ou privados. Através do mesmo instrumento, é possível que o autor pleiteie a retificação, inclusão ou supressão de dados.

Demonstrados alguns sistemas regulatórios de dados pessoais com fulcro no direito à privacidade já existentes no âmbito internacional, serão tratados, no capítulo seguinte, algumas legislações brasileiras já em vigor que protegem dados e informações dos brasileiros, bem como alguns projetos de leis em trâmite que versam especificamente sobre os dados pessoais.

## **5 PERSPECTIVAS PARA INSTITUIÇÃO DE UM SISTEMA REGULATÓRIO BRASILEIRO DE DADOS PESSOAIS**

O ordenamento brasileiro, se comparado aos demais sistemas legislativos no âmbito internacional, encontra-se um pouco atrasado quanto à proteção de dados pessoais, como forma de garantir efetivamente o direito à privacidade e à intimidade. Inclusive, é espantoso observar a situação regulatória dos países latino-americanos, que já estão bem mais a frente, com sistemas regulatórios eficazes, enquanto o Brasil não possui sequer uma lei geral de proteção de dados pessoais.

Nos últimos anos, é possível afirmar que houve uma propagação de lei gerais de proteção de dados na América Latina. Nestas há a definição dos direitos dos cidadãos, bem como a criação de mecanismos para o cumprimento destes por meio de Agências Reguladoras – verdadeiras autoridades administrativas que objetivam a proteção de dados pessoais. É possível verificar o seguinte padrão entre as normas gerais latinas: a positivação dos direitos de proteção de dados pessoais; a criação de uma autoridade administrativa; a criação de instrumentos jurídicos para garantir e proteger os dados pessoais.

O Congresso Nacional Brasileiro, por sua vez, atualmente possui alguns projetos de lei em trâmite – pode-se citar o Projeto de Lei nº 5.276/2016 da Câmara dos Deputados, que “dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural”(BRASIL 2016); bem como o Projeto de Lei nº 330/2013, do Senado Federal, que conta com a ementa: “dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências” (BRASIL, 2013).

Desta forma, inicialmente, o presente capítulo apresentará algumas legislações já existentes no ordenamento nacional, que podem servir como garantia do direito à intimidade protegendo as informações pessoais. No entanto, deve-se ressaltar de que não há nenhuma legislação brasileira específica referente a dados pessoais. Em seguida, serão estudados os projetos de lei supracitados que visam, especificamente, versar sobre um sistema regulatório dos dados pessoais dos brasileiros.

## 5.1 LEGISLAÇÃO NACIONAL DE PROTEÇÃO À INTIMIDADE COM FULCRO NAS INFORMAÇÕES PESSOAIS

A priori, cumpre mencionar a tutela originária e fundamental ao direito à privacidade e intimidade dos brasileiros, compreendida no art. 5º, inciso X, da Constituição Federal de 1988, que dispõe o seguinte: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988).

Na tentativa de o ordenamento brasileiro tutelar efetivamente o direito à privacidade e intimidade, encontram-se esparsas inúmeras normas infraconstitucionais, sendo algumas protetoras da privacidade e intimidade de forma expressa, enquanto outras tutelam tais direitos sem mencioná-los diretamente. No entanto, percebe-se que essa proteção constitucional no âmbito da privacidade e da intimidade é bastante genérica, passível das mais diversas interpretações. Inclusive o texto da Constituição não versa especificamente sobre a proteção de dados pessoais, dando margem a lacunas que não protegem especificamente tais institutos, que, conforme amplamente demonstrado, estão diretamente ligados à privacidade.

A proteção prevista no art. 21 do Código Civil (BRASIL, 2002) – verdadeiro fruto do processo de Constitucionalização e Humanização do Direito Civil – dispõe que a vida privada do indivíduo é inviolável, cabendo ao magistrado, caso requerido pelo interessado, aplicar as medidas necessárias para que se impeça ou cesse a violação. Portanto, esse dispositivo apenas confirma a vinculação e influência da tutela constitucional no âmbito do direito privado. Todavia, do mesmo modo que ocorre com a proteção constitucional da intimidade e privacidade, neste dispositivo não há proteção direta e específica para os dados pessoais, permanecendo o caráter genérico da norma, restando para o Poder Judiciário a interpretação e aplicação de tal norma quando verificar a possibilidade no caso concreto.

Entretanto, verifica-se uma menção direta no texto constitucional no que concerne à proteção de dados, pois o art. 5º, inciso XII, da Constituição de 1988 dispõe: “é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal” (BRASIL, 1988).

Sobre tema, Caio Lima e Renato Monteiro (2013, p. 62) observam uma ressalva interessante a respeito do supracitado dispositivo constitucional:

Este mandamento constitucional foi regulado pela Lei Federal nº 9.296/96 que, em seu Art. 1º, parágrafo único, afirma que a proteção dada aos sistemas de telefonia também se aplica à interceptação de fluxo de comunicações em sistemas de informática e telemática. Todavia, o texto legal, ao utilizar a palavra “fluxo de comunicações”, trouxe consigo divergência doutrinária e jurisprudencial em face da diferença entre dados estáticos e dados “em movimento”. Contudo, pelo fato da Lei nº Federal 9.472/97, conhecida como Lei Geral de Telecomunicações (LGT), conceituar telecomunicação como transmissão, emissão ou recepção de informações de qualquer natureza, apenas o fluxo de comunicações estaria protegido pelo inciso XII da CF/88 e pelo Art. 1º da Lei nº 9.296/96.

Neste sentido, apenas os dados estáticos teriam a proteção do inciso XII garantida pela privacidade – tem-se por dados estáticos, os registros eletrônicos de empresas, como os Protocolo de Internet (IP). O projeto de Lei 5.276/2016 (BRASIL, 2016), denominado de Lei de Proteção de Dados Pessoais, o qual será analisado adiante, pretende findar a divergência entre dados estáticos e dados em movimento, pois, em seu texto, afirma que dados pessoais só poderiam ser fornecidos mediante ordem judicial.

Não se pode deixar de mencionar o principal remédio constitucional relativo à proteção de dados e informações dos cidadãos brasileiros, o Habeas Data, previsto no art. 5º, inciso LXXII, alíneas *a* e *b*, da Constituição de 1988. O referido instrumento, nos termos da Constituição, pode ser utilizado em duas situações: a primeira delas se dá “para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público” (BRASIL, 1988). Em outras palavras, a Constituição garante que o indivíduo tenha a possibilidade conhecer os dados referentes ao titular, que estão armazenados em banco de dados.

Caso, após a tomada de conhecimento dos dados, o titular venha a se sentir violado, seja por sua intimidade ou privacidade, poderá postular a sua correção. A referida possibilidade está prevista na alínea *b* do mesmo dispositivo, que prevê que caberá Habeas Data “para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo” (BRASIL, 1988). Cabe mencionar o art. 7º, III, da Lei nº 9.507/97 (BRASIL, 1997), que regula o Habeas Data, que prevê uma terceira finalidade para tal instrumento, que é a possibilidade de complementação de dados, caso o titular verifique que as informações contidas no registro estejam incompletas.

O Código de Defesa do Consumidor (BRASIL, 1990) prevê também uma proteção aos dados dos consumidores, pois em seu art. 43 lhes garante o acesso às informações a seu respeito contidas em cadastros, fichas, registros, bem como os dados já arquivados. Para além disso, o parágrafo segundo do mesmo dispositivo também protege os dados pessoais dos consumidores, ao determinar que o consumidor deve ser comunicado por escrito, quando, sem solicitação sua, houver abertura de cadastro, ficha ou registro a seu respeito. No parágrafo terceiro, por sua vez, é garantido ao consumidor a imediata correção de seus dados caso encontrem-se equivocados.

Entretanto, percebe-se que as garantias previstas no art. 43 do CDC e em seus parágrafos são destinadas tão somente aos consumidores, e não uma proteção para todos acerca dos dados pessoais – até porque não deveria referir-se de maneira genérica, trata-se de um Código específico voltado às relações consumeristas. Na verdade, o referido dispositivo consumerista apenas apresenta uma reafirmação das garantias previstas nas alíneas do art. 5º, inciso LXXII, da Constituição Federal de 1988.

É possível destacar outro mecanismo nacional que visa a proteção da privacidade e da intimidade dos brasileiros no que concerne aos seus dados pessoais. Trata-se da Política Nacional de Informática, prevista na Lei nº 7.232/1984 (BRASIL, 1984), que dispõe:

Art. 2º A Política Nacional de Informática tem por objetivo a capacitação nacional nas atividades de informática, em proveito do desenvolvimento social, cultural, político, tecnológico e econômico da sociedade brasileira, atendidos os seguintes princípios:

[...]

VIII - Estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas;

IX - Estabelecimento de mecanismos e instrumentos para assegurar a todo cidadão o direito ao acesso e à retificação de informações sobre ele existentes em bases de dados públicas ou privadas;

[...].

Ora, ainda que a referida lei se comprometa em assegurar a proteção dos dados pessoais dos brasileiros, esta não fornece, de fato, os mecanismos eficazes para suprir o que determina em seus dispositivos, trazendo consigo apenas normas de conteúdo programático. Isto porque, como já demonstrado, não há ainda no Brasil uma legislação específica sobre a proteção dos dados pessoais e seu tratamento, estando a matéria ainda



em processo embrionário legislativo, havendo alguns projetos de lei que serão discorridos a seguir.

Por fim, não se pode deixar de mencionar a Lei nº 12.965/2014 (BRASIL, 2014), também conhecida como Marco Civil da Internet, que estabelece princípios gerais, direitos e deveres para o uso da internet no âmbito nacional. Em seu art. 3º, a lei dispõe sobre os princípios que devem ser respeitados durante o uso da internet, dentre eles: o princípio da proteção da privacidade (inciso II) e princípio da proteção dos dados pessoais (inciso III). Ora, de imediato, percebe-se que há um princípio norteador que garante que, no âmbito virtual, deve ser respeitada a privacidade, adotando medidas de proteção aos dados pessoais.

No entanto, seria uma utopia imaginar que a solução para todas adversidades e conflitos jurídicos do uso da internet e do ambiente cibernético está prevista na Lei nº 12.965/2014. Até porque, por exemplo, a proteção dos dados pessoais é apenas definida como uma garantia aos cidadãos brasileiros, porém não há nenhum meio de tutela adequada e específica para proteger tais dados.

Inclusive, alguns dos dispositivos previstos no Marco Civil da Internet, deixam a proteção aos dados pessoais à margem de grandes ameaças, inclusive por parte do Poder Público. Por exemplo, o art. 15 e seus parágrafos da referida Lei legaliza a retenção de dados pessoais em provedores de aplicação de internet e obtenção deles por autoridade administrativa, para fins investigativos e policiais. No entanto, o referido dispositivo não garante quais argumentos podem ser utilizados por essas autoridades (policiais, administrativas ou o próprio Ministério Público) para requerer os registros armazenados. Tem-se, ainda, que a obtenção dos registros dependerá necessariamente de ordem judicial.

Os critérios que ensejam a determinação judicial para obtenção dos registros pessoais estão previstos no art. 22, quais sejam: “fundados indícios da ocorrência de ilícito”; “justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória”; e cabível para qualquer tipo de ação judicial; “processo judicial cível ou penal, em caráter incidental ou autônomo” (BRASIL, 2014). Porém tais critérios são amplos e genéricos, o que possibilita decisões não fundamentadas, tornando a obtenção de dados a regra, e não a exceção.

Deste modo, seria interessante a criação de uma autoridade pública com a função de garantir a proteção de dados pessoais, principalmente para monitorar essas determinações judiciais, fazendo com que os magistrados elaborem fundamentações convincentes para a disponibilização dos dados pessoais. Uma Lei de Proteção de Dados deveria estipular precisamente as autoridades que teriam o poder de requerer cautelarmente a obtenção de dados pessoais, bem como deveria prever quais razões seriam justificáveis.

O Marco Civil da Internet não regulamenta o uso indevido de dados pessoais por empresas privadas, pois a mera definição de que há um “direito à proteção de dados”, como já dito, não é suficiente para garanti-lo, ou seja, positivado direitos não os torna eficazes. Portanto, ainda que todas as normas sejam relevantes e fundamentais para a proteção dos dados pessoais no Brasil, nenhuma das legislações aqui discorrida pretende ser uma norma geral aplicável à proteção de dados pessoais. Logo, ainda que proteja a privacidade e a intimidade dos brasileiros, ainda não há uma proteção eficaz, estruturada e abrangente para os dados pessoais dos brasileiros.

## 5.2 PROJETOS DE LEIS QUE VERSAM ESPECIFICAMENTE SOBRE PROTEÇÃO DE DADOS PESSOAIS

Estão em trâmite no Congresso Nacional alguns projetos de leis que visam regular a proteção de dados no âmbito nacional. Na presente seção, discorrer-se-á sobre dois, conforme já dito no início deste capítulo, o Projeto de Lei nº 5.276 de 2016 e o Projeto de Lei nº 330 de 2013.

### 5.2.1 Projeto de Lei nº 5.276/2016

O Projeto de Lei nº 5.276/2016 (BRASIL, 2016) é de autoria do Ministério da Justiça, que está em discussão pública para sua criação desde 2010. Isto porque, paralelamente à edição do Marco Civil da Internet, houve um consenso entre o Comitê Gestor da Internet, academias e demais setores governamentais, de que era necessária a criação de uma lei abrangente para tutelar os cidadãos com relação a seus dados pessoais.

A construção do referido projeto de Lei teve ampla participação social no âmbito virtual, por meio de um blog online, em que o Governo federal publicou a minuta do anteprojeto. Deste modo, houve uma mobilização da sociedade civil e empresas privadas para participar do processo de elaboração do anteprojeto.

O projeto tramita, atualmente, perante a Câmara dos Deputados, contendo aspectos relevantes para proteção dos direitos dos brasileiros que têm seus dados pessoais submetidos a um processo de tratamento, seja realizado por órgão privado ou público. O Projeto de Lei nº 5.276 recai sobre pessoas naturais ou jurídicas, seja de Direito Público ou Privado, alcançando operações de tratamento de dados que sejam realizadas em território nacional, ou que, pelo menos, a coleta dos dados ocorra no Brasil – portanto, percebe-se que não importa a localização da sede da pessoa jurídica.

O art. 5º do Projeto traz alguns conceitos iniciais e relevantes, definindo dados pessoais, dados sensíveis, dados anonimizados, dentre outros. Neste sentido, conceitua-se dado pessoal como aquele relacionado à pessoa natural, identificada ou identificável, incluindo-se dados de localização ou identificadores eletrônicos. O tratamento de dados, por sua vez, é conceituado como qualquer operação realizada que incida sobre dados pessoais, seja coleta, produção, classificação, armazenamento, entre outros.

Além disso, o mesmo dispositivo conceitua os dados sensíveis como os dados pessoais que possuam origem racial ou étnica; que carreguem as convicções religiosas, políticas, filosóficas; bem como dados referentes à saúde ou vida sexual. Traz, ainda, o instituto dos dados anonimizados, que são aqueles relativos a um titular que não pode ser identificado. Ainda que traga inúmeros outros conceitos, por fim, vale ressaltar o conceito de consentimento trazido no corpo legislativo, como a manifestação livre, informada e inequívoca através da qual o titular dos dados concorda com o tratamento destes para uma finalidade específica.

O art. 7º, §1º, dispõe que, embora seja permitido o tratamento de dados pelo o Poder Público, visando o cumprimento de obrigações legais ou execução de políticas públicas, este deverá ser sempre informado ao titular dos dados. Neste mesmo sentido, o art. 8º complementa que o acesso às informações contidas no tratamento de dados deve sempre ser facilitado ao titular, incluindo em tais informações: a finalidade específica para o tratamento, a sua forma e duração, bem como o seu responsável, dentre outras informações.

Sabe-se que, devido à internet, inúmeros processos de tratamento de dados pessoais de determinado país são realizados por outros países. Observando isso, o capítulo V do referido projeto de lei regulamenta também a transferência internacional de dados pessoais. O art. 33 prevê que a transferência de dados só poderá ocorrer com países que

possuam um nível semelhante ao brasileiro de proteção de dados, devendo ser informado ao titular dos dados o caráter internacional do tratamento de seus dados.

### 5.2.2 Projeto de Lei nº 330/2013

O Projeto de Lei nº 330 (BRASIL, 2013) é de autoria do Senado Federal, e, assim como o Projeto de Lei 5.276/2016 contém aspectos fundamentais para proteção de dados pessoais dos brasileiros.

É possível afirmar que há uma divergência em quais dados poderiam ser tutelados pelo o art. 5º, XII, da Constituição, já citado anteriormente. Neste sentido, visando pôr fim nesta divergência, o Projeto de Lei nº 330 traz uma conceituação expressa de dados pessoais, pois o art. 3º, inciso I, de forma sucinta, define dado pessoal como toda e qualquer informação relativa a pessoa identificada ou identificável.

O referido projeto tem ampla aplicação, pois pretende regulamentar as atividades que versem sobre processamento e tratamento de dados pessoais de qualquer sujeito que esteja no Brasil. Em outras palavras, a aplicação da legislação brasileira incidiria, até mesmo, sobre dados de pessoa estrangeira, que esteja no Brasil.

A supracitada conclusão retira fundamento do art. 2º do Projeto de Lei nº 330 (BRASIL, 2013), depois de alterado pela emenda nº 31, *in verbis*:

Art. 2º Esta Lei aplica-se ao uso e ao tratamento de dados pessoais realizados no todo ou em parte no território nacional ou que nele produza ou possa produzir efeito, qualquer que seja o mecanismo empregado.

§ 1º Esta Lei aplica-se:

I - Mesmo que a atividade seja realizada por pessoa jurídica sediada no exterior, desde que ofereça serviço ao público brasileiro ou pelo menos um integrante do mesmo grupo econômico possua estabelecimento no Brasil; (grifos).

No entanto, a referida disposição pode ser negativa para a sociedade brasileira, pois a legislação protecionista recairia sobre o simples trânsito de dados em território nacional – o que é de grande ocorrência, pelo caráter fluído dos dados, principalmente os virtuais. Inclusive, essa interpretação caminha em sentido contrário ao adotado pela Diretiva 95/46/CE (UNIÃO EUROPEIA, 1995), que deve ser tratada como legislação referência.

O art. 4º da Diretiva 95/46/CE (UNIÃO EUROPEIA, 1995) regulamenta a matéria da seguinte maneira:

Art. 4º.

1. Cada Estado-membro aplicará as suas disposições nacionais adoptadas por força da presente diretiva ao tratamento de dados pessoais quando:

[...]

b) O responsável pelo tratamento não estiver estabelecido no território do Estado-membro, mas num local onde a sua legislação nacional seja aplicável por força do direito internacional público;

c) O responsável pelo tratamento não estiver estabelecido no território da Comunidade e recorrer, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território desse Estado-membro, salvo se esses meios só forem utilizados para trânsito no território da Comunidade. (grifos);

Quanto aos dados sensíveis, depois de alterado pela supracitada emenda, o art. 15 do Projeto veda expressamente o seu tratamento, trazendo algumas exceções em seus incisos em que se viabilizaria o processamento de dados sensíveis. Deste modo, seria possível a realização de tal medida quando houver o consentimento expresso e específico do titular; quando for realizado para fim exclusivo de pesquisa histórica, científica ou jornalística, sem fins lucrativos, desde que sejam adicionadas medidas de proteção<sup>5</sup>; quando for necessário para tutela da saúde ou integridade física do titular ou de terceiros; dentre outros.

O consentimento do titular tem uma relevância extrema no presente projeto, pois considera-o como ponto fundamental para proteção da privacidade e intimidade. O art. 4º dispõe sobre os princípios aplicáveis ao tratamento de dados pessoais e, dentre eles, em seu inciso V, prevê que o consentimento deve ser livre, específico, inequívoco e informado do titular. Em se tratando de dados sensíveis, o mesmo inciso determina que o consentimento, além daqueles requisitos, deverá ser prévio e expresso.

O art. 13, por sua vez, prevê que o consentimento deve ser prestado pelo titular de forma separada das demais declarações, apontando uma finalidade delimitada, específica e legítima. O parágrafo terceiro deste dispositivo dispõe que o consentimento poderá ser revogado, a qualquer momento e sem ônus algum. Deve-se atentar que o termo “sem ônus” se refere a “sem custo financeiro”, ou seja, o titular poderá revogar seu consentimento gratuitamente. A este respeito, o Instituto Brasileiro de Direito Digital, na Nota Técnica nº 35 (2015, p. 10), aduz que:

---

<sup>5</sup> Nesta hipótese de exceção, seria interesse ter atenção em quais atividades seriam consideradas especificamente como atividade de pesquisa histórica, científica ou jornalística, como forma de se impossibilitar que atividades meramente comerciais utilizem tal dispositivo como escusa de aplicação da legislação, ou seja, como forma de evitar que aleguem que estão enquadrados nesta exceção.

A distinção é extremamente relevante, pois em diversos negócios jurídicos celebrados online, o tratamento de dados pessoais é justamente o que possibilita o fornecimento de serviços e de conteúdo gratuito, custeado por meio de anúncios publicitários direcionados ao titular que utiliza um determinado serviço ou acessa determinado conteúdo. Esse é, inclusive, o modelo de negócios padrão na Internet na atualidade. Nesse contexto, tal como dito acima em relação à oposição do titular ao tratamento de seus dados pessoais, é importante compreender que a revogação do consentimento pode acarretar no cancelamento de determinado serviço online ou na impossibilidade de acesso a determinado conteúdo.

É possível encontrar uma convergência entre o Projeto nº 330/2013 e o Marco Civil da Internet, quanto às sanções aplicadas nas hipóteses de violação das disposições de cada lei. Isto porque, o art. 30 do Projeto e o art. 12 do Marco Civil da Internet, dispõem de forma semelhante que, sem prejuízo das sanções cíveis, criminais, ou administrativas, aqueles que agirem desconformidade com a respectiva legislação estará sujeito a:

- Advertência (inciso I de ambos os artigos);
- Multa de certa porcentagem do faturamento do grupo econômico com estabelecimento no Brasil (inciso III do Projeto, determinando 5% de multa, inciso II da Lei, determinando 10% de multa);
- Suspensão das atividades de tratamento de dados pessoais (inciso IV do Projeto, que determina suspensão total ou parcial, e inciso III da Lei, que determina apenas suspensão temporária);
- Proibição das atividades de tratamento de dados pessoais (inciso V do Projeto, que determina proibição total ou parcial, e inciso IV da Lei, que determina a proibição do exercício).
- Ainda, o Projeto nº 330/2013 acrescenta duas outras sanções, quais sejam: a alteração, retificação ou cancelamento do banco de dados, bem como a intervenção judicial.

Percebe-se que em nenhum dos projetos de lei estudados há a previsão da criação de um órgão regulatório ou autoridade garantidora dos direitos à proteção dos dados pessoais dos cidadãos brasileiros. Na verdade, no anteprojeto da Lei nº 5.276/2016 havia a previsão de uma tutela administrativa, através da criação de um Conselho Nacional de Proteção de Dados, que possuiria autonomia administrativa e orçamentária, com função de Autoridade de Garantia à proteção de dados pessoais e monitoramento do setor privado e público.

No entanto, durante a discussão do anteprojeto, houve forte mobilização do setor privado e empresarial contra a criação da referida Autoridade, sob o argumento de que já existem órgãos que poderiam exercer a referida função, dentre os quais: o PROCON, o Ministério Público, entre outros. Deste modo, acabou que nenhum dos projetos de lei institui um órgão público específico e independente com função de proteger os dados pessoais, o que levanta algumas preocupações quanto a efetividade de tais leis.

Inclusive, importante ressaltar que, conforme a ARTIGO19 (2016, p. 45):

A ausência de um órgão independente levanta sérias preocupações sobre as possibilidades da lei ser implementada consistentemente e efetivamente sobre todos os setores. Cerca de 90% das leis de proteção de dados ao redor do mundo possuem uma autoridade independente para proteção de dados. São dois os principais problemas resultantes da ausência de um órgão independente. Primeiramente, os titulares dos dados serão abandonados com o ônus da iniciativa, sem a expertise adequada, e tendo que enfrentar uma distribuição desigual de interesses, pois estão limitados à iniciativa individual. Em segundo lugar, como resultado, o tempo para que a lei se torne efetiva será muito mais longo, tomando um tempo maior para que os princípios e as mesmas medidas se tornem claros para que tenham algum impacto preventivo.

Todas as legislações e projetos de lei expostos no presente trabalho foram tratados de forma sintética, até porque uma pormenorização de cada lei seria além do razoável para o que propõe este estudo. No entanto, mesmo diante de certa brevidade na explanação, é cristalina a relevância da proteção dos dados pessoais e da entrada em vigor de tais projetos de lei, devendo estes correr em urgência constitucional, como forma de dar brevidade na tutela das garantias fundamentais dos cidadãos brasileiros.

Isto porque, ainda que haja proteção por aquelas legislações supracitadas, que já estão vigentes, não há no ordenamento Brasil uma norma geral de proteção de dados pessoais, como ocorre em outros países do estrangeiro. Os projetos, embora com algumas falhas, caminham para a criação da referida norma geral, o que deve ser tratado com urgência e relevância, como já dito, devido ao caráter fluído e a presença constante dos dados pessoais na vida cotidiana dos brasileiros.

Além disso, deve-se ter em mente que o Brasil deve tutelar o processamento, armazenamento e transmissão de dados sem, contudo, violar a liberdade de informação, de circulação de ideias, entre outras garantias do Estado Democrático e de Direito que se vive no Brasil. Logo, seria razoável considerar como solução ponderada uma responsabilização maior daqueles que são detentores dos provedores que transmitem, processam e armazenam dados pessoais, sem prejuízo de responsabilização do autor da infração de forma subjetiva, seja pessoa física ou jurídica. Deste modo, é fácil de se

constatar que a legislação brasileira procura se dedicar a proteção dos direitos à privacidade e à intimidade, porém, em razão das inúmeras maneiras de violação a estes direitos já existentes em sociedade, ainda há um longo percurso para garantir maior efetividade à tutela de tais direitos e garantia à proteção dos dados pessoais.



## 6 CONCLUSÃO

O direito à privacidade vê-se acuado diante da atual sociedade da informação. Atestou-se, por meio do presente estudo, a necessidade de se contribuir com a comunidade através de melhores interpretações para a aplicação do direito à privacidade e à intimidade, sendo considerada todas as dimensões de tal instituto diante desse novo cenário social, político e econômico que está sendo instaurado em todo o globo.

Deste modo, é necessária a instauração de medidas administrativas e, principalmente, legislativas, que visem promover efetivamente a garantia constitucional à privacidade, mesmo diante de tantos avanços tecnológicos e, especificamente, à frente das tecnologias da informação. Faz-se fundamental a conscientização popular quanto aos riscos a que se sujeita o direito à privacidade ante tais avanços tecnológicos, sobretudo no que tange ao tratamento e processamento de dados pessoais por meio dos sistemas automatizados.

Inicialmente, fora demonstrada a nova perspectiva do Direito Civil Constitucional Humanizado, compreendendo através desta concepção os direitos da personalidade previstos no ordenamento brasileiro. Como resposta da constitucionalização do Direito Privado no que concerne à proteção da personalidade, verifica-se a existência da Cláusula Geral da Personalidade. Tal cláusula determina que todas as decisões que versem sobre direito à personalidade devem ser tomadas com prioridade à pessoa humana e a sua dignidade.

Em seguida, pontuou-se cada direito da personalidade previsto no Código Civil, como forma de situar o leitor, dando-lhe uma compreensão abrangente onde está inserido o direito à privacidade no ordenamento jurídico brasileiro. Neste diapasão, entende-se por privacidade a possibilidade dada aos sujeitos de direito de obstar a intromissão em sua vida particular, além de ser compreendida como forma de impedir o acesso e divulgação das informações a seu respeito. A doutrina conta com a Teoria das Esferas para distinguir a privacidade e a intimidade que, embora semelhantes, possuem algumas divergências entre si. Dentre elas, tem-se que a privacidade é mais abrangente, de modo que o titular opta por compartilhar algumas informações para pessoas a sua escolha, enquanto a intimidade é a mais restrita, resguardando o indivíduo as informações apenas para si.

A atual sociedade que vivemos pode ser denominada de sociedade da informação, que é uma nova maneira de organização social embasada em uma intensa utilização de

meios tecnológicos para fins de armazenamento, produção e transmissão de dados e informações. Esta nova organização social afeta diretamente no direito à privacidade, pois os dados e informações são objetos imediatos de proteção da privacidade.

Com isso, é possível afirmar que os dados são considerados como informações em potencial, pois depois de comunicado ou compreendido é que se tornará uma informação completa. Já os dados pessoais são aqueles que versem sobre circunstâncias de cunho pessoal de um sujeito identificado ou identificável. Os dados sensíveis, por sua vez, são considerados como uma nova categoria de dados pessoais, que são aqueles que possuem conteúdo íntimo do titular, ou seja, podem versar sobre opção sexual, religião, saúde – uma vez utilizados indevidamente, podem possuir conteúdo altamente discriminatório. Um exemplo de processamento e tratamento de dados sensíveis são os registros médicos, os quais podem conter problemas de saúde, sequência de genes, entre outros.

No âmbito consumerista algumas técnicas de armazenamento e processamento de dados são utilizadas, dentre elas: *data warehouse*, *data mining*, *profiling* e *scoring*. A *data warehouse* é um sistema de armazenamento de informações em grande quantidade; *data mining* é um sistema de mineração de dados, em que dados de difícil compreensão são transformados em informações úteis; *profiling* é a reunião de dados sobre a mesma pessoa a fim de construir um perfil de um sujeito específico; *scoring* é um sistema de avaliação de sujeitos, em que são separados em bons e maus consumidores.

Diante do desenvolvimento tecnológico, que viabilizou das mais diversas maneiras de violação da privacidade e intimidade dos sujeitos, através do processamento de dados, alguns países instituíram modelos regulatórios para proteção de dados pessoais de seus cidadãos.

As legislações europeias são as mais influentes no âmbito internacional, no que concerne a proteção de dados pessoais, que passaram a surgir a partir da década de 70. Neste sentido, a doutrina traça algumas gerações das leis do referido continente sobre o tema. A primeira geração tem um viés funcional, de modo que o funcionamento do banco de dados dependerá de licença prévia dos titulares dos dados. A segunda geração, por sua vez, ultrapassa o mero cuidado com procedimentos, para ter um viés protecionista do direito à privacidade de forma imediata. A terceira geração, na verdade, foi uma reinterpretação das normas já existentes na Europa, pois passou-se a entender que, para

garantir à privacidade dos titulares, era necessário permitir a sua participação integral no processamento de seus dados. Por fim, a quarta geração intensificou, ainda mais, a participação do titular, determinando inclusive que alguns dados não poderiam sair do seu controle, que são os dados sensíveis.

Os modelos regulatórios que foram tomados como exemplo para o presente estudo foram o europeu, o norte-americano e o uruguaio. O primeiro é o modelo mais tradicional e possui uma abordagem personalista dos direitos fundamentais, enquanto que o segundo está na contramão, pois possui um viés libertário, ou seja, está pautado nos princípios da liberdade contratual e da propriedade privada. O modelo uruguaio é tomado para estudo por conter forte influência do modelo tradicional europeu, mas com algumas adaptações para a realidade da América Latina.

Quanto ao ordenamento brasileiro, é possível afirmar que este se encontra atrás dos ordenamentos internacionais, no que concerne a proteção de dados pessoais. Isto porque, ainda não há uma norma geral brasileira para proteção de tais dados visando a garantia do direito fundamental à privacidade. De todo modo, os brasileiros contam com a proteção do art. 5º, inciso X, da Constituição, que protege a intimidade e a privacidade dos brasileiros, bem como o art. 21 do Código Civil, que dispõe no mesmo sentido, determinando que a vida privada é inviolável. No entanto, ambos os dispositivos possuem caráter genérico, protegendo a privacidade e a intimidade de forma ampla e genérica.

Atualmente, corre no Congresso Nacional projetos de lei que visam proteger à privacidade e intimidade com relação a proteção e regulação dos dados pessoais dos brasileiros, dentre os quais foram citados o Projeto de Lei 5.276/2016 e Projeto de Lei 330/2013, do Ministério da Justiça e do Senado Federal, respectivamente.

Conclui-se, portanto, que o atual estado em que se encontram os aparatos tecnológicos, bem como a grande possibilidade de coleta de dados dos indivíduos, permitindo o conhecimento completo sobre a vida de cada um – muitas vezes sem a anuência do titular – não permite que haja um cenário apático quanto à proteção dos dados pessoais dos indivíduos, nomeadamente os brasileiros. Isto porque, uma legislação que meramente conceitua a privacidade, de forma abrangente e elástica – como a que existe hodiernamente –, não se demonstra suficiente para evitar lesões e abusos à privacidade e à intimidade do cidadão.

## REFERÊNCIAS

ARTIGO 19. **Proteção de dados pessoais no Brasil: Análise dos projetos de lei em tramitação no Congresso Nacional**, 2016. Disponível em: <<http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>>. Acesso em: 24 set. 2017.

BOFF, Salete Oro; FORTES, Vinícius Borges. **A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental**: perspectivas de construção de um marco regulatório para o Brasil. 2014. Disponível em: <[http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S2177-70552014000100006](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2177-70552014000100006)>. Acesso em: 13 set. 2017.

BORTOLINI, Ana Carolina dos Santos. **Administração de banco de dados e a violação do direito à privacidade**: paradoxos e tendências. Monografia (Graduação) – Universidade Federal do Rio Grande do Sul. Departamento de Ciências Administrativas, Porto Alegre, 2012.

BRASIL. Código Civil. **Lei nº 10.406 de 10 de janeiro de 2002**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/2002/L10406.htm](http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm). Acesso 7 set. 2017.

\_\_\_\_\_. Código de Defesa do Consumidor. **Lei nº 8.078 de 11 de setembro de 1990**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/L8078.htm](http://www.planalto.gov.br/ccivil_03/leis/L8078.htm). Acesso em: 24 set. 2017.

\_\_\_\_\_. **Constituição da República Federativa do Brasil de 1988**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em 7 set. 2017.

\_\_\_\_\_. **Lei nº 7.232 de 29 de outubro de 1984**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/L7232.htm](http://www.planalto.gov.br/ccivil_03/leis/L7232.htm). Acesso em: 24 set. 2017.

\_\_\_\_\_. **Lei nº 9.507 de 12 de novembro de 2017**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/L9507.htm](http://www.planalto.gov.br/ccivil_03/leis/L9507.htm). Acesso em: 03 set. 2017.

\_\_\_\_\_. **Lei nº 12.965 de 23 de abril de 2014**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm). Acesso em: 24 set. 2017.

\_\_\_\_\_. **Projeto de Lei nº 330 de 2013**. Disponível em: <http://legis.senado.leg.br/sdleg-getter/documento?dm=2931559&disposition=inline>. Acesso em: 01 out. 2017

\_\_\_\_\_. **Projeto de Lei nº 5276 de 2016**. Disponível em: [http://www.camara.gov.br/proposicoesWeb/prop\\_mostrarintegra?codteor=1457459&filename=PL+5276/2016](http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016). Acesso em: 01 out. 2017

\_\_\_\_\_. Senado Federal. **Quadro comparativo do Projeto de Lei nº 330, de 2013**. Brasília. 2017. Disponível em: <http://legis.senado.leg.br/sdleg-getter/documento?dm=5111559&disposition=inline>. Acesso em: 01 out. 2017

\_\_\_\_\_. Tribunal Superior do Trabalho. Acórdão nº 532006120035090091. Claudemir Bombonato. Employer - Organização de Recursos Humanos Ltda. e Rurícula Agenciamento de Mão-de-obra Rural Ltda. Relator: Ministra Maria de Assis Calsing.

Brasília, DF, 02 de abril de 2008. **Diário Eletrônico da Justiça do Trabalho**. Brasília, 18 abr. 2008.

CASTRO, Catarina Sarmento e. **Direito da Informática, Privacidade e Dados Pessoais**. Coimbra: Almedina, 2005.

CONSELHO EUROPEU. In: WIKIPÉDIA, a enciclopédia livre. Flórida: **Wikimedia** Foundation, 2017. Disponível em:  
<[https://pt.wikipedia.org/w/index.php?title=Conselho\\_Europeu&oldid=49503805](https://pt.wikipedia.org/w/index.php?title=Conselho_Europeu&oldid=49503805)>.  
Acesso em: 9 ago. 2017.

DONEDA, Danilo. **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. 2011. Disponível em:  
<http://www.egov.ufsc.br/portal/conteudo/considera%C3%A7%C3%B5es-iniciais-sobre-os-bancos-de-dados-informatizados-e-o-direito-%C3%A0-privacidade>. Acesso em: 24 set. 2017.

\_\_\_\_\_, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

ENUNCIADO nº 6 do CJF/STJ, da **I Jornada de Direito Civil**, 2002. Disponível em:  
<http://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/EnunciadosAprovados-Jornadas-1345.pdf>. Acessado em 03 set. 2017.

ESTADOS UNIDOS DA AMÉRICA. Electronic Communications Privacy Act, 18 U.S.C. §2510 e ss., **Public Law**, Washinton D.C., 21 out. 1986.

\_\_\_\_\_. Health Insurance Portability and Accountability Act, 110 Stat. 1936, **Public Law**, Washinton D.C., 21 ago. 1996.

\_\_\_\_\_. Privacy Act, 88 Stat. 1896, **Public Law**, Washinton D.C., 31 dez. 1974.

FAUSTINO, André. A proteção de dados pessoais no Brasil: Breve histórico do direito comparado até a atual realidade brasileira. In: **Âmbito Jurídico**, Rio Grande, XIX, n. 154, 2016. Disponível em: <[http://www.ambito-juridico.com.br/site/index.php?n\\_link=revista\\_artigos\\_leitura&artigo\\_id=18241&revista\\_caderno=17](http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=18241&revista_caderno=17)>. Acesso em: 07 set. 2017.

FRANÇA. **Lei nº 78-77** da Assembleia Nacional e Senado de 6 de janeiro de 1978, relativa à proteção de informações, ficheiros e liberdades. Disponível em:  
<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>. Acesso em 03 out. 2017.

GONÇALVES, Andrey Felipe Lacerda; BERTOTTI, Monique; MUNIZ, Veyzon Campos. O direito fundamental à privacidade e à intimidade no cenário brasileiro na perspectiva de um direito à proteção de dados pessoais. **Revista de Direito Privado**, Rio Grande do Sul, p.45-62, 2013.

GONÇALVES, Maria Eduarda. **Direito da informação**: novos direitos e modos de regulação na sociedade da informação. Coimbra: Almedina, 2003, pg. 89.

GUERRA, Sidney. **O direito à privacidade na internet**: uma discussão da esfera privada no mundo globalizado. Rio de Janeiro: América Jurídica, 2004.

GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. [2017]. Disponível em: <<https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>>. Acesso em: 16 set. 2017

INSTITUTO BRASILEIRO DE DIREITO DIGITAL. **Nota técnica n. 35 de 2015**. Brasília. 2015. Disponível em: [http://docs.wixstatic.com/ugd/d43cf3\\_7d5194ff19294eb4a9599766495691b0.pdf](http://docs.wixstatic.com/ugd/d43cf3_7d5194ff19294eb4a9599766495691b0.pdf). Acesso em 04 out. 2017

LIMA, C. C. C.; MONTEIRO, R. L. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. **AtoZ: novas práticas em informação e conhecimento**, Curitiba, v. 2, n. 1, 2013.

LIMA, Caio Cesar Carvalho; MONTEIRO, Renato Leite. **Panorama brasileiro sobre a proteção de dados pessoais**: discussão e análise comparada. 2013. Disponível em: <<http://revistas.ufpr.br/atoz/article/view/41320/25260>>. Acesso em: 24 set. 2017.

MADRID, Fulgencio. **Derecho a la intimidad, informática y Estado de Derecho**, Valencia, Universidad de Valencia, 1984.

MAIA, Luciano Soares. **A privacidade e os Princípios de proteção do indivíduo perante os bancos de dados pessoais**. [1993]. Disponível em: <[http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/bh/luciano\\_soares\\_maia.pdf](http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/bh/luciano_soares_maia.pdf)>. Acesso em 26 jul. 2017.

MARTINS, Leonardo (org). **Cinquenta anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideu. Fundação Konrad Adenauer, 2005, p. 244-245.

MAYER-SCHÖNBERGER, “Generational Development of Data Protection in Europe”. In: **Technology and Privacy: The New Landscape**. Massachusetts: The MIT Press, 2001.

MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. 158 f. Dissertação (Mestrado) - Curso de Direito, Departamento de Pós-graduação, Universidade de Brasília, Brasília, 2008.

OMBUDSMAN. In: WIKIPÉDIA, a enciclopédia livre. Flórida: **Wikimedia** Foundation, 2017. Disponível em: <<https://pt.wikipedia.org/w/index.php?title=Ombudsman&oldid=48352037>>. Acesso em: 01 out. 2017

ORWELL, George. **1984**. São Paulo: Companhia das Letras, [1949]. Tradução de: Alexandre Hubner, Heloísa Jahn.

PINTO, Cristiano Otávio Paixão Araújo. **Reação norte-americana aos atentados de 11 de setembro de 2001 e seu impacto no constitucionalismo contemporâneo**: Um estudo a partir da Teoria da Diferenciação do Direito. 2004. 424 f. Tese (Doutorado) - Curso de Direito, Universidade Federal de Minas Gerais, Belo Horizonte, 2004.

RABELO, Iglesias Fernanda de Azevedo; GARCIA, Filipe Rodrigues. O direito à autodeterminação informativa. In: **Âmbito Jurídico**, Rio Grande, XIV, n. 93, 2011. Disponível em: <http://www.ambito->

juridico.com.br/site/index.php?n\_link=revista\_artigos\_leitura&artigo\_id=10473. Acesso em: 21 ago. 2017.

REINALDO FILHO, Demócrito Ramos. **Responsabilidade por publicações na Internet**. Editora Forense. Rio de Janeiro, 2005.

ROSA, Tais Hemann da; FERRARI, Graziela Maria Rigo. **Privacidade, intimidade e proteção de dados pessoais**. 2014. Disponível em: <[http://seer.uenp.edu.br/index.php/argumenta/article/viewFile/495/pdf\\_69](http://seer.uenp.edu.br/index.php/argumenta/article/viewFile/495/pdf_69)>. Acesso em: 10 set. 2017.

SANTOS, Marcelo Pereira dos. Os direitos da pessoa humana na concepção civil-constitucional: uma releitura da tutela da personalidade. In: I CONGRESSO INTERNACIONAL DE DIREITOS DA PERSONALIDADE, 1., 2014, Maringá. **Anais...**. Maringá: Unicesumar, 2014. p. 1 - 26. Disponível em: <[http://www.cesumar.br/prppge/pesquisa/mostras/pri\\_mestrado/pdf/07\\_GT1\\_Marcelo\\_Pereira\\_Santos.pdf](http://www.cesumar.br/prppge/pesquisa/mostras/pri_mestrado/pdf/07_GT1_Marcelo_Pereira_Santos.pdf)>. Acesso em: 18 ago. 2017.

TEPENDINO, Gustavo (Coord.). **O código civil na perspectiva civil-constitucional**. Rio de Janeiro: Renovar, 2013.

UNIÃO EUROPEIA. **Convenção de 108 de 28 de janeiro de 1981** para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em 09 ago. 2017

\_\_\_\_\_. Decisão 2001/497/CE da Comissão das Comunidades Europeias, de 15 de junho de 2001, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros, nos termos da Diretiva 95/46/CE. **Jornal Oficial das Comunidades Europeias**. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32001D0497&from=PT>. Acesso em 27 set. 2017.

\_\_\_\_\_. Diretiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas. **Jornal Oficial das Comunidades Europeias**. Bruxelas, 12 de julho de 2002. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:pt:PDF>. Acesso em 07 set. 2017.

\_\_\_\_\_. Diretiva 95/46/CE do Parlamento Europeu e do Conselho da Europa, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**. Portugal, 23 de novembro de 1995. Disponível em: [http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46\\_part1\\_pt.pdf](http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf). Acesso em 07 set. 2017.

\_\_\_\_\_. Regulamento n° 679 de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. **Jornal Oficial das Comunidades Europeias**. Portugal, 27 de abril de 2016. Disponível em: <https://publications.europa.eu/pt/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-pt>. Acesso em 04 out. 2017.

URUGUAI. Decreto nº 414 de 2009. **Diario Oficial**, Montevideo, 31 ago. 2009.

Disponível em:

[https://www.google.com.br/search?q=%22Decreto+n%C2%BA+414%22+uruguai&oq=%22Decreto+n%C2%BA+414%22+uruguai&gs\\_l=psy-ab.3...10927.14423.0.14678.5.5.0.0.0.199.668.0j4.4.0....0...1.1.64.psy-ab..1.0.0....0.ezzEksVokmw](https://www.google.com.br/search?q=%22Decreto+n%C2%BA+414%22+uruguai&oq=%22Decreto+n%C2%BA+414%22+uruguai&gs_l=psy-ab.3...10927.14423.0.14678.5.5.0.0.0.199.668.0j4.4.0....0...1.1.64.psy-ab..1.0.0....0.ezzEksVokmw). Acesso em 04 out. 2017.

\_\_\_\_\_. Decreto nº 396 de 2003. **Diario Oficial**, Montevideo, 30 de outubro de 2003.

Disponível em:

<http://www.redipd.org/documentacion/legislacion/common/legislacion/uruguay/decreto-396-003.pdf>. Acesso em: 04 out. 2017.

\_\_\_\_\_. Decreto nº 249 de 2007. **Diario Oficial**, Montevideo, 09 de julho de 2007.

Disponível em:

<http://www.redipd.org/documentacion/legislacion/common/legislacion/uruguay/decreto-249-007.pdf>. Acesso em 04 out. 2017.

\_\_\_\_\_. Lei nº 18.331 de 2008 sobre a Proteção de dados pessoais e a ação de ‘Habeas Data’. **Diario Oficial**, Montevideo, 18 ago. 2008. Disponível em:

<https://legislativo.parlamento.gub.uy/temporales/leytemp3461501.htm>. Acesso em 04 out. 2017.

VALDETARO, Úrsula Brandão Faria. **Utilização de dados pessoais em serviços financeiros**. 2017. 69 f. TCC (Graduação) - Curso de Direito, Universidade de Brasília, Brasília, 2017.

VIEIRA, Alexandre Pires; RALVES, Cláudio. O direito à privacidade frente aos avanços tecnológicos na sociedade da informação. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 19, n. 3979, 2014. Disponível em: <<https://jus.com.br/artigos/27972>>. Acesso em: 03 set. 2017.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. 2007. 297 f. Dissertação (Mestrado) - Curso de Direito, Universidade de Brasília, Brasília, 2007.